Graduado en Ingeniería Informática

Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros Informáticos

TRABAJO FIN DE GRADO

Creación y automatización de laboratorios configurables CCNA Cisco para la realización de prácticas de networking.

Autor: Alejandro Plaza Arralde

MADRID, ENERO DE 2015

ÍNDICE

1. RESUMEN

El presente trabajo está enfocado a facilitar la realización de prácticas con equipamiento de laboratorio físico, permitiendo que se tenga acceso a diferentes escenarios virtuales (topologías de ejercicios) sin necesidad de variar la configuración física (conexionado) de dos kits de laboratorio oficial para CCNA Routing & Switching[1] y CCNA Security[2]. Para ello se plantea la creación de diferentes escenarios o topologías virtuales que puedan montarse sobre el mismo escenario de conexionado físico.

Es necesario revisar y seleccionar los ejercicios prácticos más destacados en términos de importancia de las curriculas de CCNA Routing & Switching y CCNA Security. Naturalmente, estos ejercicios han de variar en sus interfaces, nomenclatura y documentación para que cuadren con las especificaciones disponibles del laboratorio físico, todo ello sin perder nada de su fundamento.

Los escenarios físicos deben de ser lo más versátiles posibles para dar soporte a las topologías requeridas en los ejercicios prácticos de los cursos oficiales de CISCO CCNA Routing & Switching y CCNA Security, con el objetivo de realizar los mínimos cambios de configuración física posibles, y poder simultanear la realización de diferentes prácticas y entre alumnos de diferentes asignaturas. También se pretende posibilitar que los profesores desarrollen sus propios ejercicios prácticos compatibles con el conexionado físico escogido. Para ello se utilizará un servidor de acceso (Access Server) para que los alumnos puedan configurar de forma remota los diferentes equipos sin necesidad de acudir en persona al laboratorio, aunque esta también sea una opción más que viable. Los dos escenarios contarán con tres routers, tres switches y un firewall, de forma que han sido montados en su respectivo armario, al igual que sus conexiones y cableado.

La deshabilitación de puertos en los diferentes equipos de red que forman el kit de laboratorio (routers, switches y firewalls) dará lugar a los diferentes escenarios virtuales. Se crearán VLANs en los switches para establecer diferentes conexiones. Estos escenarios deberán ofrecer la variedad necesaria para realizar las diferentes prácticas necesarias en las asignaturas “Tecnologías de Red CISCO: CCNA” [3], “Redes y Comunicaciones” [4] y “Diseño y Seguridad de Redes” [5].

Además, para facilitar y agilizar el cambio entre topologías, se debe automatizar la configuración básica de cada escenario virtual (activación/desactivación de puertos) en base a la topología deseada, y el establecimiento de una configuración inicial. De forma que los alumnos puedan comenzar los ejercicios de igual forma a lo que ven en los documentos explicativos, y en el caso de terminar su sesión (o cerrarla voluntariamente) que sus progresos en el mismo se guarden para posteriores sesiones de forma que puedan proseguir su tarea cuando deseen.

2. SUMMARY

The present work is aimed at facilitating the experiments with equipment Physical Laboratory, allowing access to different virtual scenarios (topologies exercises) without changing the physical configuration (connection) with two kits of official laboratory for CCNA Routing & Switching[1] and CCNA Security[2]. This requires the creation of different scenarios or virtual topologies that can be mounted on the same physical connection scenario arises.

It is necessary to review and select the most prominent practical exercises in terms of importance of curricula of CCNA Routing and Switching, and CCNA Security. Naturally, these exercises must vary in their interfaces, nomenclature and documentation available that fit the specifications of the physical laboratory, all without losing any of its foundation.

The physical setting should be as versatile as possible to support topologies required in the practical exercises of official courses CISCO Routing and Switching CCNA, and CCNA Security, in order to make the minimum possible changes in physical configuration, and can simultaneous realization of different practices, and between students of different subjects. It also aims to enable teachers to develop their own practical exercises compatible with the physical connection chosen. For this, we will use an Access Server will be used by the students to access remotely to configure different computers without having to go in person to the laboratory, but this is also an other viable option. The two scenarios have three routers, three switches and a firewall, so that have been mounted in their respective rack, as well as their connections and wiring.

Disabling ports on different network equipment that make up the lab kit (routers, switches and firewalls) will lead to different virtual scenarios. These scenarios should provide the variety needed to perform the necessary practices in different subjects "Network Technologies CISCO: CCNA"[3], "Networking and Communications"[4] and "Design and Network Security." [5]

Moreover, to facilitate and expedite the exchange topologies, it was necessary to automate the basic configuration of each virtual setting (on/off ports) based on the desired topology, and the establishment of an initial configuration. So that, the students can begin the exercises equally to what they see on explanatory documents, and if they finish their session (or close voluntarily) their progress on the exercise will be saved for future sessions so that they can continue their work when they want.

3. INTRODUCCIÓN

Este trabajo está orientado a facilitar la realización de prácticas con equipamiento de laboratorio físico, permitiendo que los usuarios o alumnos tengan acceso a diferentes escenarios virtuales, es decir, diferentes tipologías basadas en ejercicios reales de la asignatura impartida en la Escuela Técnica Superior de Ingenieros Informáticos[6] "Tecnologías de Redes: Cisco", sin necesidad de variar la configuración física y cambiar las conexiones de un kit de laboratorio oficial para CCNA Routing & Switching o CCNA Security, accediendo de forma remota.

El trabajo ha sido propuesto por Miguel Jiménez Gañán [7], Doctor en Informática por la Universidad Politécnica de Madrid [8] e Ingeniero en Informática por la misma universidad. El proyecto ha sido realizado dentro del contexto del Laboratorio de Redes de Computadores [9] y Tecnologías Web (CoNWeT Lab) [10].

En primera instancia, será necesario la elección y revisión de los numerosos ejercicios de los que disponen los cursos oficiales de CISCO CCNA Routing & Switching y CCNA Security que puedan cuadrar con la topología física disponible establecida en el laboratorio de la facultad. De esta forma se buscan ejercicios prácticos que tengan un alto contenido educativo en la asignatura, para que los alumnos puedan reforzar sus conocimientos, mediante su respectiva práctica de los mismos. Al haber cursado la asignatura recientemente no es un problema destacar los aspectos más importantes del curso de CCNA Routing & Switching, no obstante el temario correspondiente a la certificación CCNA Security sí ha requerido de una mayor atención al tener una gran carga conceptual sobre seguridad no contemplada en dicha asignatura. Una vez elegidas las topologías virtuales adecuadas, se debe generalizar todas sus topologías con el fin de simplificar el proceso de creación de una topología común a todas ellas que encaje en el modelo establecido en el laboratorio físico. De esta forma, se intentó crear el menor número de topologías, partiendo de una por cada ejercicio y terminando con sólo una global que cuadrará los requisitos de todas las anteriores, siendo necesario modificar la documentación de algunos ejercicios cambiando algunas de sus interfaces de sus Switches y Routers, para que se adapten a la topología física, y única, del laboratorio y las nuevas topologías creadas virtualmente, estas últimas realizadas mediante la herramienta Cisco Packet Tracer [11].

Los dos kits de laboratorio físicos configurados, pese a contar con los mismos equipos y configuración, deberán admitir diversidad de topologías virtuales, por lo que es necesario que éste pueda cambiarse físicamente en poco tiempo con el fin de que los alumnos puedan realizar los ejercicios de los cursos oficiales de CISCO CCNA Routing & Switching y CCNA Security tanto de forma virtual como física. Para ello, se tendrá un Access Server con el que se podrán configurar los equipos de forma remota sin necesidad

de estar físicamente en el laboratorio, siendo esta una de las claves del trabajo. Para una configuración desde cero de los equipos, es necesario acceder por consola a este Access Server, lo cual implica presencia física junto al equipo, algo también necesario en el caso de contar con alguna incidencia grave.

El laboratorio constará de dos kits de laboratorio, como se ha apuntado anteriormente, cada uno compuesto por tres routers 2911 CISCO2911/K9 [12], uno de los cuales, el de arriba, tiene características de seguridad CISCO2911-SEC/K9 [13], tres switches 2960 de 24 puertos WS-C2960-24TT-L [14], un firewall ASA 5505 ASA5505-BUN-K9 [15], además del Access Server común, para configurar ambos escenarios de forma remota. Esto es, un punto de entrada que permite a los usuarios o clientes acceder a una red y está destinado a actuar como una puerta de entrada para proteger el acceso a un recurso protegido, en este caso los dos kits de laboratorio. Como se ha mencionado anteriormente, para configurar los equipos se requiere acceder por consola a este Access Server, el cual tiene 16 conexiones asíncronas disponibles mediante un OCTAL-ASYNC-CABLE que conectamos a cada puerto de consola de los 7 equipos de los dos kits disponibles, usando conexiones SSH para acceder a cada uno y poder configurarlo.

De igual forma, tomando como referencia las topologías virtuales escogidas y las restricciones físicas del laboratorio, todas las conexiones y la totalidad del cableado deben de ser realizadas desde cero, por lo que resulta vital realizar multitud de cables, tanto cruzados como directos, para el correcto funcionamiento e implementación de las topologías.

Con el fin de agilizar la puesta en marcha de los laboratorios y minimizar el número de escenarios físicos será necesario establecer una configuración general global para el conexionado físico. Además, para cada topología virtual se debe automatizar una configuración inicial adecuada a su documentación, activando o desactivando las interfaces necesarias para la realización de todos y cada uno de los ejercicios. Asimismo, con el fin de guardar el trabajo realizado por los alumnos, se establecerán *backups* [16] o copias de seguridad para que una vez cerrada la sesión los progresos queden guardados hasta la próxima sesión o la próxima vez que el alumno decida abrir esa topología.

El trabajo finaliza como punto de partida para que otro compañero del departamento haga su Trabajo fin de Grado. Realizando la aplicación web correspondiente mediante la cual los alumnos puedan acceder a los ejercicios virtuales, los cuales son simulados en el laboratorio físico instalado. De esta forma la comunicación entre ambos alumnos y tutores ha resultado fundamental para coincidir en algunos aspectos comunes a la hora de decidir las tecnologías y lenguajes a utilizar, al igual que el número de topologías disponible o las restricciones del laboratorio físico.

Los objetivos principales del Trabajo de Fin de Grado son los siguientes:

- Revisión y elección de los ejercicios de los cursos CISCO CCNA Routing & Switching y CCNA Security que puedan adaptarse a las características del laboratorio físico, al igual que a las competencias de las asignaturas que requerirán de su utilización.
- Instalación del kit de laboratorio físico (routers, switches y firewalls) y su cableado de red con el fin de emular las configuraciones virtuales que se encuentran en la currícula de los cursos CISCO CCNA Routing & Switching y CCNA Security adaptándose a los ejercicios previamente elegidos.
- Crear, si es posible un escenario, o varios, que pueda acoger todas las topologías de los ejercicios, y sus correspondientes escenarios virtuales, que se correspondan con topologías de ejercicios prácticos elegidos previamente de los cursos CISCO CCNA Routing & Switching y CCNA Security que se imparten en la facultad.
- Lograr la máxima fidelidad y aprovechamiento de cada escenario en función de los ejercicios de CCNA Routing & Switching y de CCNA Security, respetando los requisitos de cada ejercicio, mostrando al usuario la configuración de igual forma que la de sus enunciados.
- Será necesario guardar y automatizar diferentes configuraciones en función de los ejercicios que los alumnos deseen realizar, con el fin de que los usuarios puedan retomar su trabajo en posteriores sesiones sin perder progreso alguno en sus laboratorios o ejercicios. Para ello se deberá automatizar la configuración básica inicial de los equipos del laboratorio en función del ejercicio elegido por parte del alumno, debiendo activar o desactivar los puertos necesarios para crear la topología requerida por el propio alumno.
- Servir de nexo a la hora de añadir este trabajo a la aplicación web final que recibirán los alumnos que deseen reforzar sus conocimientos.

La memoria se dividirá en diferentes secciones que abarcan con mayor detalle la explicación y fundamento del trabajo. Tras el resumen de la anterior sección, en castellano e inglés, y de esta "Introducción", se explicarán los "Trabajos Previos de la Memoria", es decir, en líneas generales la forma en la que se aborda el trabajo (métodos y técnicas, herramientas utilizadas y posibles alternativas dentro del contexto).

Tras este punto, comienza el grueso del trabajo con su desarrollo dividido por diferentes secciones que representan los diferentes objetivos y tareas establecidas durante el "Plan de Trabajo" del mismo. En primer lugar se detallará el proceso de revisión y elección de los ejercicios de los cursos CISCO CCNA Routing & Switching y CCNA Security, su respectiva elaboración de las diferentes topologías virtuales y la instalación del kit de laboratorio físico. La memoria continúa con la Configuración del Access Server, mediante la cual se podrá acceder a los equipos y realizar sus respectivas configuraciones,

copias de seguridad y automatizaciones de las mismas. Por último, una breve explicación del proceso de añadir todo este contenido a la aplicación web que realiza otro compañero del laboratorio, pese a no ser un aspecto fundamental de mi trabajo.

Finalizando la memoria se tendrán en cuenta los resultados finales obtenidos, las conclusiones y una opinión personal de la experiencia vivida a la hora de hacer el trabajo y lo que me ha aportado a mi formación.

Cerrarán la memoria los apartados de anexos y la correspondiente bibliografía del trabajo.

4. TRABAJOS PREVIOS DE LA MEMORIA

Este trabajo se basa en ofrecer a los diferentes alumnos de las asignaturas “Redes de Computadores” y “Tecnologías de Redes: Cisco”, impartidas en la Facultad de Informática, la posibilidad de poder acceder desde sus propios ordenadores personales a los diferentes ejercicios prácticos que engloban los temarios de las asignaturas para poder así afianzar sus conocimientos. De esta forma, el proyecto llega como una necesidad de los profesores titulados del Laboratorio de Redes de Computadores y Tecnologías Web (CoNWeT Lab) de la Facultad, los cuales creen necesaria la creación de una herramienta adicional a las proporcionadas por las asignaturas y su temario, para que los alumnos mejoren sus conocimientos, y por ende, sus calificaciones.

Así, como se ha explicado en los apartados anteriores de Introducción y Resumen, el trabajo comienza con ya varias decisiones tomadas al respecto por parte de los profesores del departamento, mi tutor incluido, con el fin de orientar de la mejor forma la inicialización de este trabajo.

En primer lugar se facilitaron la totalidad de los ejercicios pertenecientes a los cursos de CISCO CCNA Routing & Switching, incluyendo sus cuatro módulos que veremos con mayor detalle en próximos capítulos, y CCNA Security, los cuales serían revisados y seleccionados de forma adecuada. Para elegir estos ejercicios se utilizarían herramientas comunes de documentación como Microsoft Word [17], Microsoft Excel [18], y para hacer algunas modificaciones visuales, un programa de edición de imágenes, sirviendo el simple y conocido Paint [19] de Windows.

Asimismo, se detallaron las especificaciones del laboratorio físico, porque obviamente seleccionar topologías de ejercicios sin saber de cuantos equipos dispondría el laboratorio no tenía sentido. El laboratorio físico cuenta con dos escenarios, cada uno de ellos formado por tres routers 2911 CISCO2911/K9, uno de los cuales, el de arriba, tiene características de seguridad CISCO2911-SEC/K9, tres switches 2960 de 24 puertos WS-C2960-24TT-L y un firewall ASA 5505 ASA5505-BUN-K9. Con esta información ya se podían seleccionar los ejercicios sin problemas.

De igual forma, el laboratorio cuenta con un Access Server que se utiliza para configurar de forma remota los anteriores equipos, sin necesidad de requerir de un ordenador y un cable de consola para configurar cada equipo, no obstante en sus primeros usos es un procedimiento que se utilizará, hasta conseguir su funcionamiento remoto.

También, se establecieron una serie de restricciones a la hora de instalar el laboratorio físico, como la posición y nomenclatura de los equipos, los caminos que seguirían las

conexiones y la forma en la que se realizarían los respectivos cables cruzados y directos con las diferentes categorías de cableado disponibles.

De los ejercicios seleccionados, y tomando las restricciones establecidas, se utiliza el software de Cisco, Packet Tracer, para crear de forma virtual las topologías elegidas y asó poder apreciar posibles cambios y facilitar el montaje del laboratorio. Esta herramienta además servirá para probar los ejercicios, configuraciones y posibles aspectos de utilidad para el funcionamiento del laboratorio. Asimismo, la sintaxis utilizada por este programa será la usada para configurar los equipos. Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en el currículum de CCNA. Soporta los siguientes protocolos:

- HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS.
- TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6.
- RIP, EIGRP, OSPF Multiárea, enrutamiento estático y redistribución de rutas.
- Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP.
- ARP, CDP, STP, RSTP, 802.1q, VTP, DTP y PAgP, Polly Mkt.

Recursos, actividades y demostraciones disponibles:

- OSPF, IPv6, SSH, RSTP, Frame Relay, VLAN's, Spanning Tree, Mike mkt etc.

El lenguaje utilizado por Cisco Packet Tracer es el lenguaje textual IOS mediante la línea de comandos CLI disponible en cada equipo, en el que se van a realizar todas las configuraciones de los diferentes equipos del laboratorio. Este formato también sirve para configurar y hacer los *backups* o copias de seguridad, en total 7, una por cada equipo; ya sean las configuraciones iniciales de cada práctica virtual o el progreso guardado de cada alumno en las mismas.

El Access Server cuenta con una tarjeta NM-16ª [20], que es la que permite conectar dos cables OCTAL-ASYNC-CABLE [21] para conectar, cada cable, a 8 puertos de consola RJ-45 [22], una interfaz física comúnmente usada para conectar redes de cableado estructurado Así, se puede conectar un cliente al Access Server mediante puerto de consola con el fin de realizar su configuración básica y establecer las conexiones SSH al resto de los equipos para poder acceder de forma remota a los mismos. SSH [23] (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. La seguridad también se implementa en el Access Server, siendo necesario establecer las pautas de seguridad en el mismo para autenticar y autorizar a los alumnos que deseen

acceder a los escenarios. Obviamente, los alumnos tendrán una serie de privilegios sobre los equipos para realizar las prácticas, teniendo casi plenos poderes sobre ellos; mientras que por el contrario, no tendrán permisos de administración sobre el Access Server con el fin de salvaguardar los aspectos de seguridad, entre otros, Al ser un router CISCO, nuestro Access Server permite contar con diferentes opciones de seguridad como la gestión de diferentes líneas asíncronas, la creación de usuarios y grupos de usuarios con distintos privilegios y el filtrado de conexiones mediante la creación y configuración de ACLs [24][37][55][56] (Listas de Control de Acceso) utilizadas en el equipo.

Este trabajo sirve de nexo a otro compañero del departamento que realizará la aplicación web de dicho trabajo, en la que los alumnos podrán reservar horas para acceder al laboratorio de forma remota. La conexión principal entre ambas labores sucede en el Access Server, el cual se ha configurado de forma que el otro alumno del departamento pueda acceder de forma remota a los equipos mediante conexión SSH para la realización de su aplicación. Igualmente, se han establecido los parámetros de seguridad, como los permisos, privilegios y listas de acceso permitidas, necesarios en los equipos para que los alumnos, dados previamente de alta en la aplicación, puedan acceder mediante SSH al laboratorio y realizar sus actividades correspondientes.

Para la comunicación con los tutores será necesario la utilización de Google Docs [25] y la plataforma para compartirlos de Google Drive[26], servicio de almacenamiento de archivos, de forma que todo el equipo pueda acceder rápidamente al mismo contenido.

4.1 DOCUMENTACIÓN EXTRA

Se han encontrado algunos trabajos y proyectos similares sobre los que he podido comprender de mejor forma los objetivos y las posibles pautas de cara a la realización de este trabajo. La empresa AFORTIC [27] proporciona a los alumnos una experiencia de formación de alta calidad a través de la interacción remota con routers reales, switches, firewalls, PCs y servidores; todos ejecutando sistemas operativos reales y software; esta herramienta es similar a lo que espera conseguir el departamento con este trabajo, aunque es más guiado y no está orientado a CCNP como el que hemos conseguido hacer en la Facultad.

El TEC de Monterrey cuenta con un proyecto de "Mejora al Proceso de Enseñanza-Aprendizaje Mediante el Acceso Remoto a Laboratorios de Redes" [28] que se sirve del NETLAB [29], otra herramienta de corte similar realizada por la Universidad Nacional Abierta y a Distancia UNAD que permite a los usuarios acceder mediante su usuario y contraseña a una serie de laboratorios, siempre y cuando, cuenten con la asignación de un tutor.

Naturalmente, CISCO propone una gran cantidad de documentación acerca de sus equipos y los diferentes comandos que pueden ser utilizados, siendo de suma importancia a la hora de realizar este trabajo.

5. DESARROLLO DEL TRABAJO

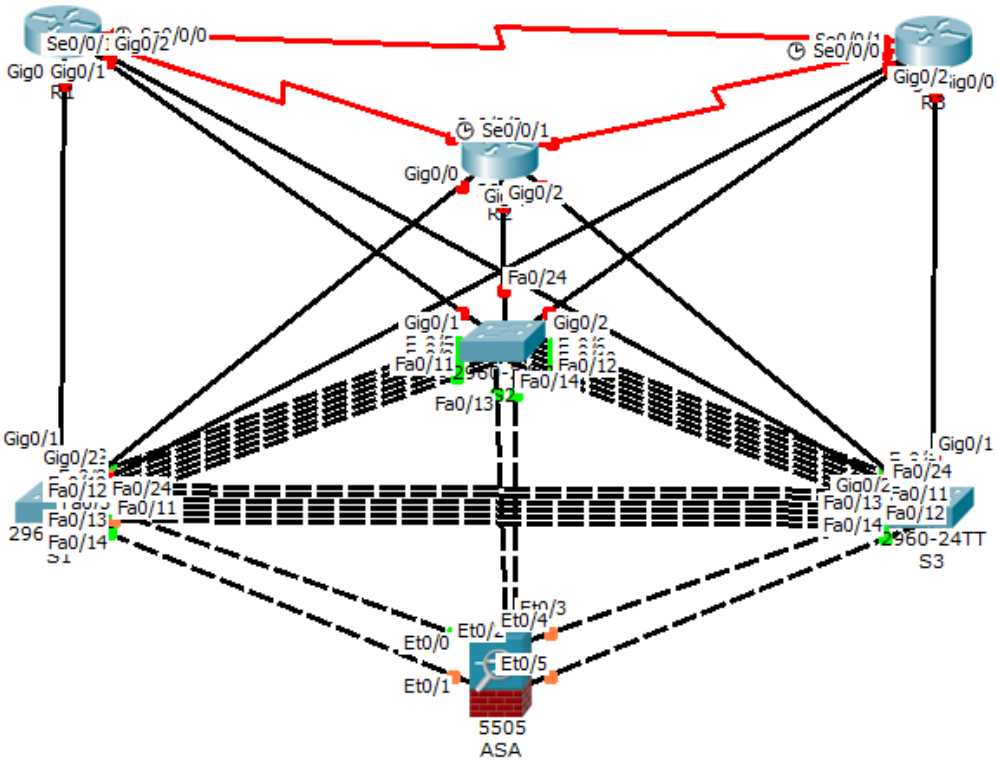
5.1 ELABORACIÓN DE LAS TOPOLOGÍAS VIRTUALES

Para la realización de esta tarea ha sido necesario recopilar toda la información obtenida de los ejercicios a elegir (detallados en la siguiente tarea) y las restricciones impuestas por los profesores acerca del kit de laboratorio físico, el cual se visitó en primera instancia para planificar las topologías, establecer una serie de pautas a seguir y facilitar posteriormente la adaptación de los ejercicios a las mismas. Con ello, se sacaron las siguientes conclusiones:

- La colocación de los switches utilizados en el laboratorio físico en secuencia, es decir, el primer switch encima del segundo, y éste encima del tercero. Esta situación obliga a crear un anillo de un anillo entre los switches, de 6 cables, por ejemplo, cogiendo fa0/1-12 en todos ellos. Las interfaces impares del S1 se deberán conectar con las pares del S3. Las pares del S1 con las impares del S2, y las pares de S2 con las impares de S3, de forma que queda lo más eficiente posible desde el punto de vista físico como virtual para facilitar su montaje y cableado.
- Los puertos serie de los 3 routers se han decidido mantener, su nomenclatura original de los ejercicios tanto los DCE como los DTE, para facilitar la comprensión de la totalidad de los enunciados y topologías, de forma que los cambios a realizar en los mismos sean lo mínimo posibles.
- Se utilizan 6 de los 8 puertos del ASA para conectar 2 a cada switch, en concreto con las interfaces FastEthernet0/13 y FastEthernet0/14.
- Se ha decidido conservar el nombre de los routers, siempre que se refiriesen originalmente como R1, R2 y R3. Cuando esto no ha sucedido se han tomado de izquierda a derecha, excepto algunas ocasiones en las que sólo hay dos de ellos y se han tomado como R1 y R3. Como siempre esto se hace a fin de simplificar las configuraciones físicas y virtuales.
- Se ha determinado que las conexiones entre los routers y switches se realicen a través de dos puertos Giga Ethernet, es decir el S1 se conectará a R2 y R3 mediante estas dos interfaces, y al igual sucede con S2 y R1-R3 y con S3 y R1 y R2, siendo el puerto FastEthernet0/24 de cada switch el que se conecte con su respectivo router, es decir S1 con R1, S2 con R2 y S3 con R3.
- Cada router debe estar conectado al resto de routers mediante conexiones serie y a la totalidad de los switches por conexión GigaEthernet.
- Se ha establecido que los equipos se conecten a los switches a través de la interfaz FastEthernet0/15 de los switches, esto a nivel virtual. No obstante, a nivel físico no existe ningún PC conectado a estos switches, por lo que será necesario a nivel virtual remoto realizar pings extendidos para comprobar la conectividad.

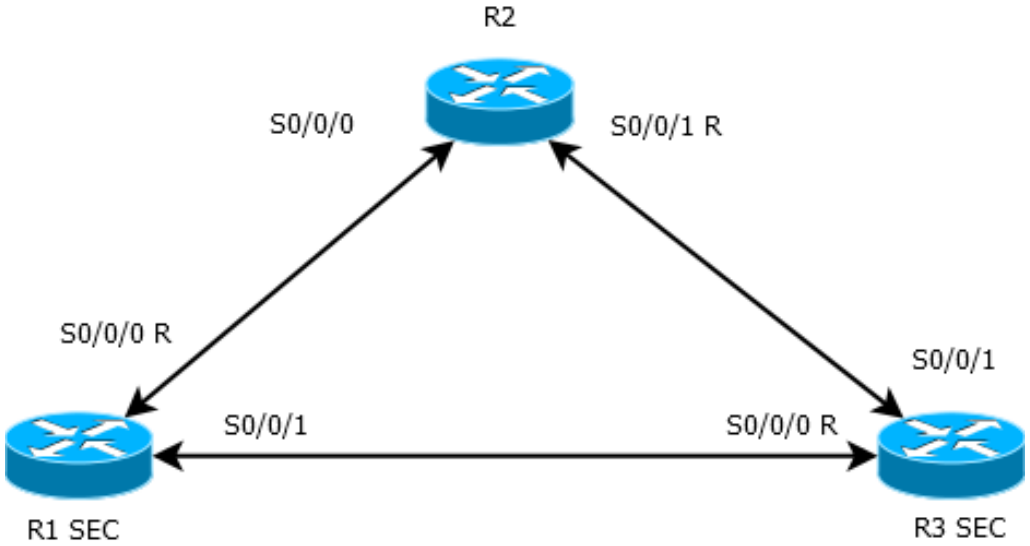
El ping extendido de Cisco no necesita parámetros o una dirección en la línea de comandos. El usuario escribe "ping" y después pulsa "Intro" para que le muestre una serie de preguntas, permitiendo escribir la dirección a la que queremos que se realice ese ping. En nuestro caso, las direcciones de los PCs que aparecen en los ejercicios pero que no se encuentran en el laboratorio físico se pueden simular estableciendo sus ips en alguna de las interfaces del router o el switch al que están conectados según los ejercicios. Así, los alumnos podrán hacer ping a la dirección de la interfaz como si se tratara de un PC, siempre previo aviso en los respectivos enunciados para que traten de esta forma los PCs existentes.

Bajo estas restricciones, se creó una topología física mediante la herramienta Cisco Packet Tracer que representara todos estos aspectos. Esta topología es la final resultante de todo el trabajo, aunque se mostrará alguna correspondiente a momentos previos e intermedios, esta es la topología final que tiene el laboratorio físico. A continuación, la topología:



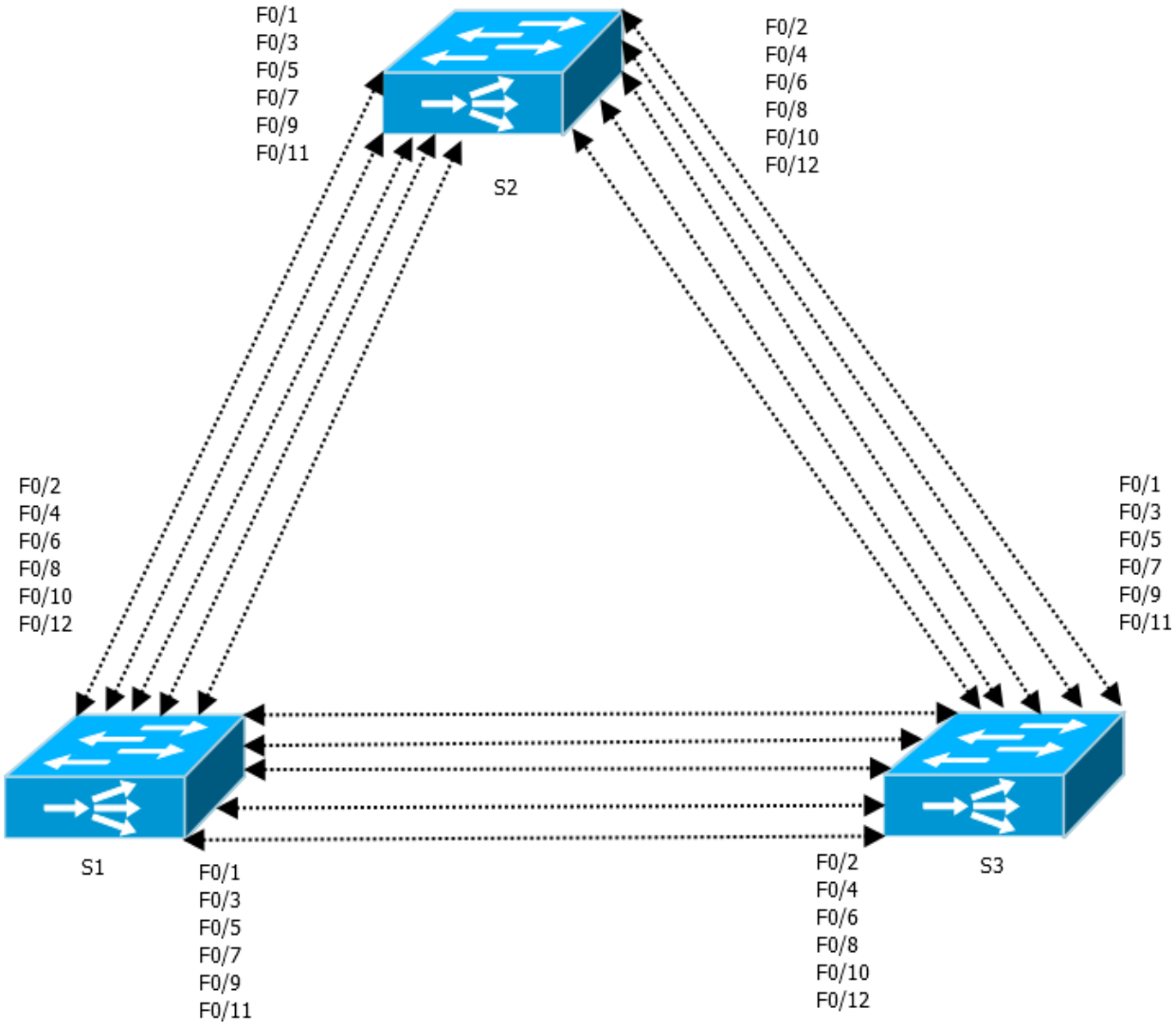
Topología final

Debido a que la anterior imagen puede llevar a confusión al no ver con precisión la totalidad de las interfaces, se han creado tres imágenes mediante la herramienta DIA que conforman todas juntas la anterior topología. En primer lugar se muestran las conexiones serie entre lo Routers, destacando R1 y R3 con características de seguridad. La 'R' de las conexiones serie significa que es la que establece la velocidad de reloj.



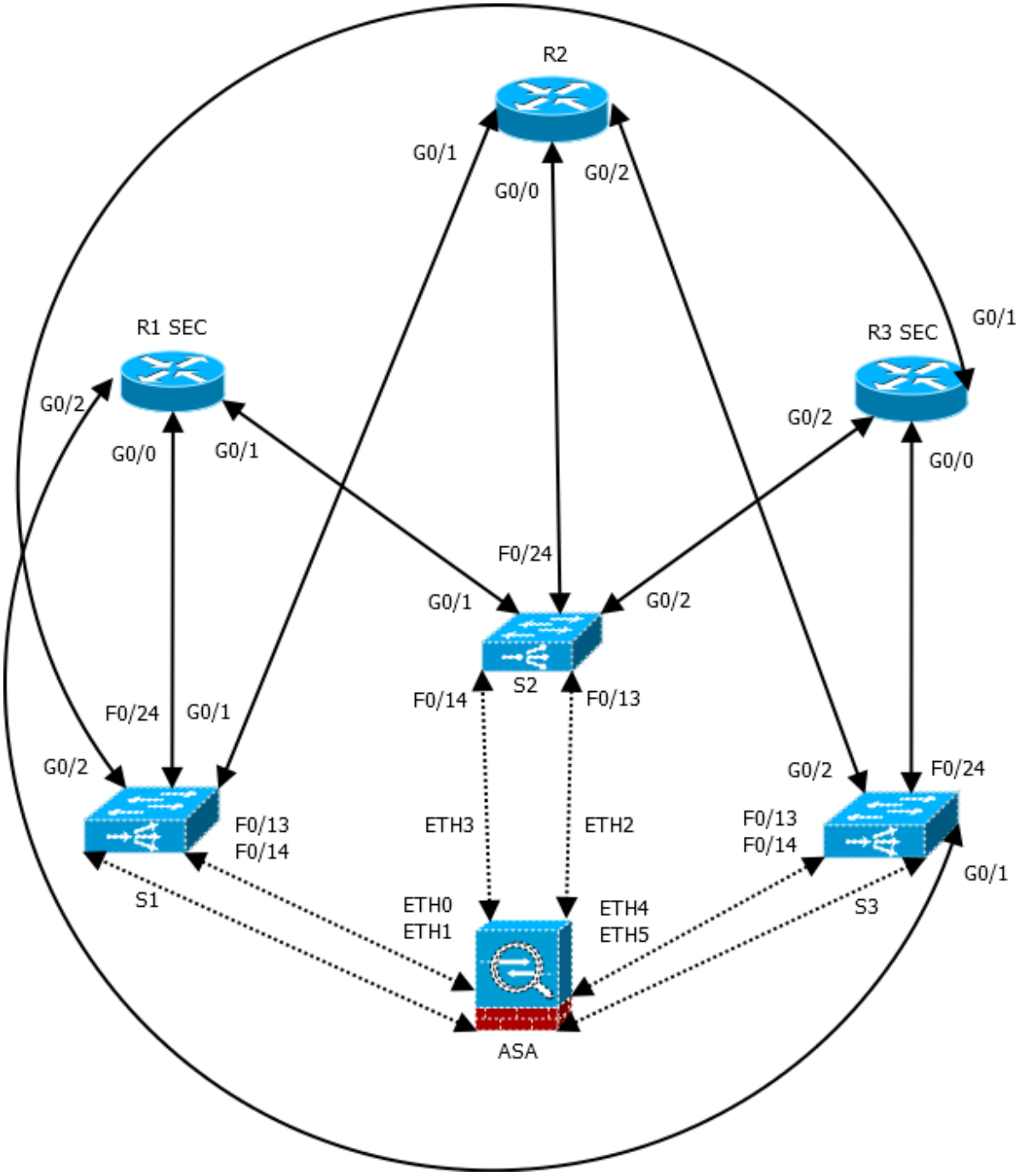
Topología final – Routers conexiones serie

En la siguiente imagen se muestran las conexiones que tienen entre sí los Switches.



Topología Final – Switches conexiones entre propios Switches

La siguiente imagen muestra las conexiones entre el ASA y los Switches, entre estos últimos y los Routers, y también se muestran las 3 VLANs que se han creado:

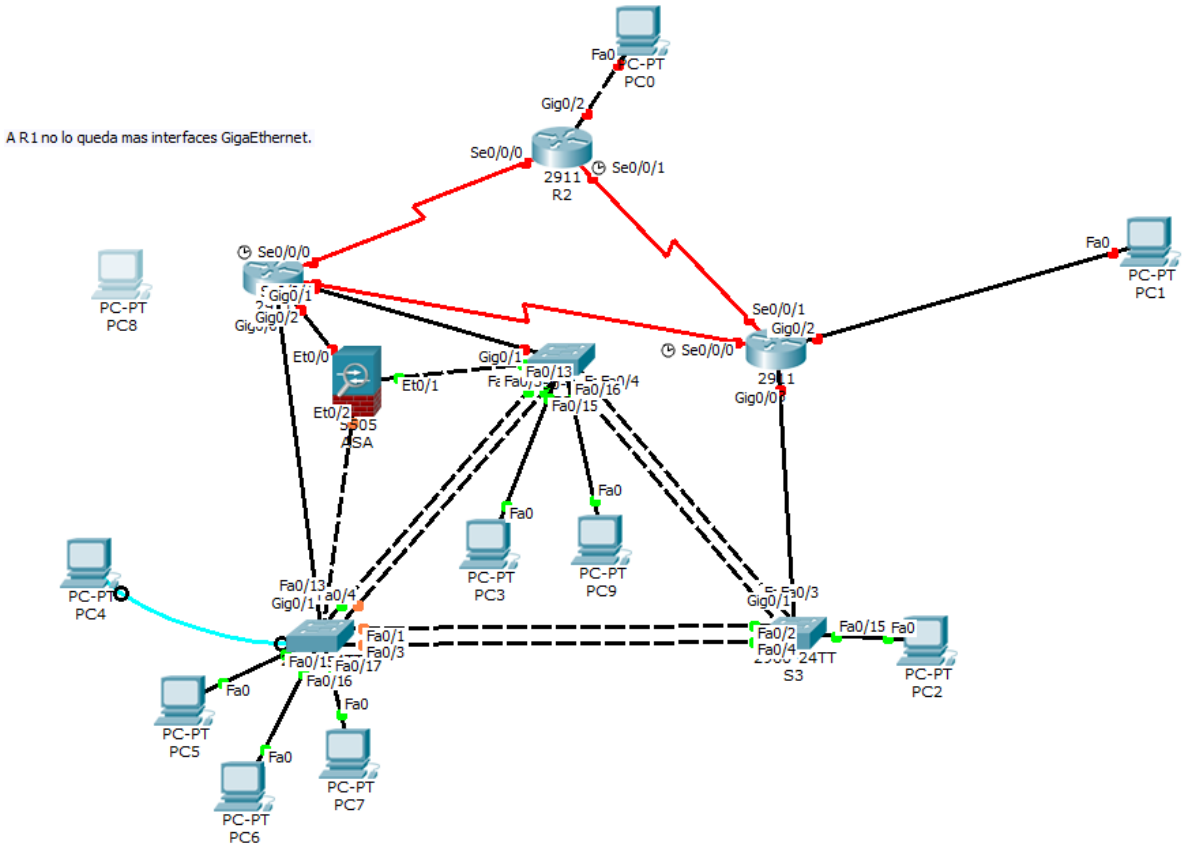


Topología Final – Switches, Routers y ASA.

Se reservan 3 identificadores de VLANs (95, 96 y 97) en cada switch con el fin de utilizarlas cuando se requiera conectar de forma indirecta cualquiera de los routers con el ASA a través de la conexión entre el router y el switch y de este último al ASA. Por

ejemplo, acceder al ASA desde cualquier router yendo al switch 1 y de ahí al ASA por la conexión Eth0, (R1-SW1-ASA).

Por otra parte, se realizó otra topología física, anterior a la final, con la misma herramienta que recogía todos los elementos vistos en los ejercicios seleccionados. En parte, esta topología fue adaptándose poco a poco a la del laboratorio, de forma que al final, el laboratorio físico pudiera montarse y respetar ambas topologías. A continuación los equipos máximos necesarios según los ejercicios seleccionados:



Topología mínima exigida según los ejercicios

- R1 se conecta a S1, S2, el firewall y los otros dos routers.
- R2 a los otros dos routers y a un posible PC.
- R3 se conecta a S3, a los otros dos routers y a un posible PC.
- S1 tiene dos conexiones con S2 y con S3, además de R1, el firewall y 4 posibles PCs, uno de ellos por consola.
- S2 tiene dos conexiones con S1 y con S3, además de R1, el firewall y 2 posibles PCs.
- S3 tiene dos conexiones con S1 y con S2, además de R3 y un posible PC.
- El firewall se conecta a R1, S1 y S2.

Esta topología suma los requisitos de todos los ejercicios seleccionados, por lo que la topología real, final de laboratorio que hemos visto antes, da cabida a los mismos y a los requisitos exigidos por los profesores o por el propio diseño físico vistos en la anterior topología.

5.2 REVISIÓN Y ELECCIÓN DE LOS EJERCICIOS DE LOS CURSOS CISCO CCNA ROUTING & SWITCHING Y CCNA SECURITY

A continuación se detallarán los ejercicios elegidos de ambas curriculas, viendo sus principales objetivos y características. De igual forma, se explicará la importancia de los mismos dentro del temario y los cambios realizados respecto a su forma original.

Los principales cambios entre las topologías originales y las modificadas son los siguientes, teniendo en cuenta la topología física final diseñada en base al laboratorio:

- La nomenclatura de los switches se cambia a S1, S2 y S3, y la de los routers a R1, R2 y R3, siendo R1 y R3 los que cuentan con características de seguridad.
- En las topologías se toman los equipos de izquierda a derecha para realizarles su respectivo cambio de nomenclatura. En el caso de haber solamente dos de los tres equipos se toma el equipo 1 y 3, ya sea el switch o el router implicado.
- Entre las restricciones físicas aplicadas a estas topologías, los switches utilizan sus primeros 12 puertos fast Ethernet para conectarse entre ellos, de forma que los pares del S1 se conectan a los impares del S2, los pares del S2 a los impares del S3, y los pares del S3 a los impares del S1.
- Las conexiones FastEthernet del 13 al 24 quedan libres para conectar PCs o el ASA (Firewall) a los switches, en nuestro caso para la topología física final el ASA en la FastEthernet 0/13-14 y el 24 con su respectivo router, quedando el resto libres.
- Las direcciones de Loopback se han ordenado de forma que comiencen en la 0 y aumenten de una en una.
- Los Routers usan la conexión Giga Ethernet 0/0 para conectarse a los switches, mientras que los switches hacen uso de la Giga Ethernet 0/1. Los Routers usan la conexión Giga Ethernet 0/2 para conectarse directamente a posibles PCs. Esto en lo que se refiere a los ejercicios, no obstante, la topología física final no contempla PCs, estando todos los puertos GigaEthernet de los Routers conectados cada uno a un switch diferente. Para solucionar este pequeño conflicto, se reserva el puerto FastEthernet 0/15 de los switches para simular un PC, aunque físicamente no exista.
- Las conexiones serie entre los routers se han acordado de la siguiente forma: R1 usa S0/0/0 DCE para conectar a R2 y R2 a R1 con S0/0/0. De R2 a R3 se usa S0/0/1 DCE y de R3 a R2 S0/0/1. De R3 a R1 se usa S0/0/0 DCE y de R1 a R3 S0/0/1.

Empezamos por los ejercicios correspondientes a CCNA Routing and Switching de su primer módulo, los cuales sirven de introducción a la herramienta Cisco Packet Tracer para los alumnos, con comandos como ping, tracert o traceroute. Además pueden repasar la creación de subredes.

El segundo módulo establece nuevos conceptos como establecer las configuraciones básicas de los equipos, configurar acceso mediante SSH [30], creación y gestión de VLANs, protocolos de encaminamiento como RIP y OSPF, y configuración de listas de acceso (ACLs) y DHCP.

El tercer módulo profundiza en nuevos conceptos de las VLANs y los protocolos de encaminamiento vistos en el anterior módulo.

El cuarto, y último módulo, correspondiente a CCNA Routing and Switching introduce PPP, FrameRelay, NAT dinámica y estática, y la creación de túneles.

Los ejercicios seleccionados de CCNA Security permiten establecer las configuraciones básicas de seguridad de los equipos, la utilización de AAA [31] [32], su acceso administrativo mediante contraseñas y líneas SSH, la monitorización de las posibles incidencias y un acercamiento a los firewalls.

5.2.1 MÓDULO 1, “INTRODUCTION TO NETWORKS”

- Ejercicio 8.3.2.7 Prueba de conectividad de red con ping y traceroute.

Objetivos:

Parte 1: Construir y configurar la red

- Realizar cableado.
- Configurar los PCs.
- Configurar los routers.
- Configurar los switches.

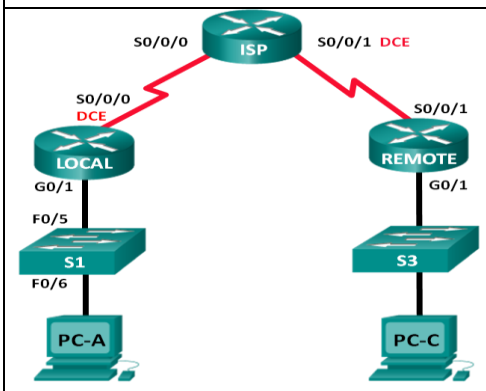
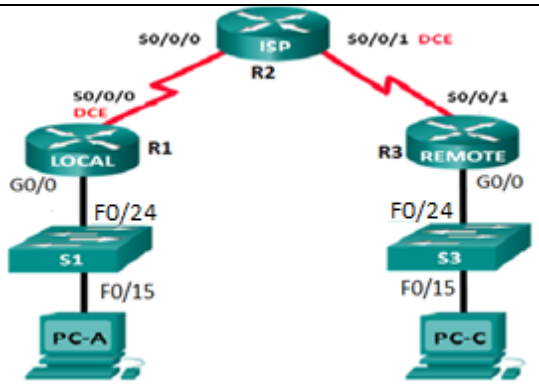
Parte 2: Usar el comando ping para probar la conectividad

- Usar ping desde un PC.
- Usar ping desde un dispositivo Cisco.

Parte 3: Usar los comandos tracert y traceroute para probar la conectividad

- Usar tracert desde un PC.
- Usar traceroute desde un dispositivo Cisco.

Parte 4: Probar la topología completa

Imagen Original	Imagen Nueva
	
Se han cambiado las diferentes interfaces de los equipos y sus nomenclaturas.	
Se ha decido introducir este ejercicio como toma de contacto para los alumnos. De esta forma se relacionarán con los primeros dispositivos cisco, sus configuraciones básicas y probarán comandos de suma utilidad como ping, tracert y traceroute.	

- Ejercicio 9.2.1.3 Diseño e implementación de un esquema de direccionamiento IPv4 dividido en subredes.

Objetivos:

Parte 1: Diseñar un esquema de subredes

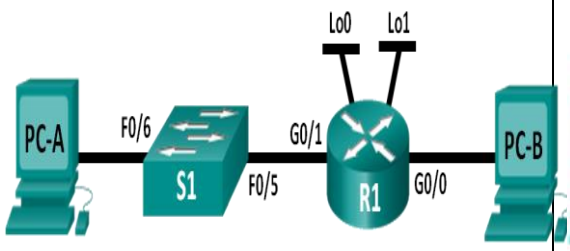
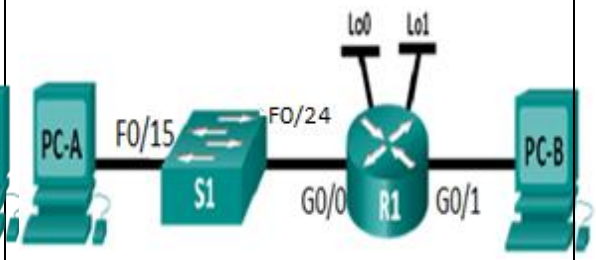
- Crear un esquema de subredes que cuadre en el número de subredes y hosts requeridos.
- Completar el diagrama con las direcciones ip dadas para los host.

Parte 2: Configurar los equipos

- Asignar una dirección ip, mascara de subred y Gateway por defecto a los PCs.
- Configurar las interfaces Gigabit Ethernet con una dirección ip y máscara de subred.
- Crear dos interfaces de loopback en el router y configurar cada una con su dirección ip y máscara de subred.

Parte 3: Probar la topología completa

- Verificar la conectividad usando el comando ping.

Imagen Original	Imagen Nueva
	
Se han cambiado las diferentes interfaces de los equipos.	
Este ejercicio va más allá, familiarizando a los alumnos con las subredes, las máscaras de subred y los loopback.	

5.2.2 MÓDULO 2 “ROUTING AND SWITCHINF ESSENTIALS”

- Ejercicio 2.1.1.6 Configuración de los parámetros básicos de un switch.

Objetivos:
Parte 1: Realizar cableado y verificar la conectividad y la configuración básica por defecto del Switch.
Parte 2: Configurar los parámetros básicos de red de los equipos.

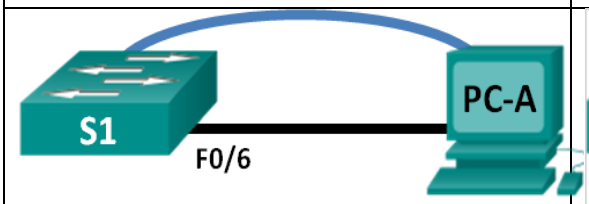
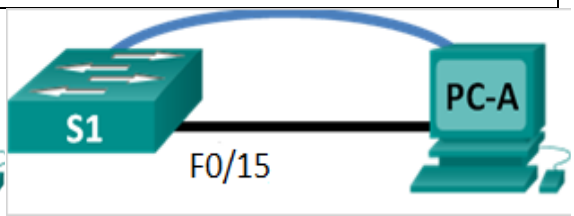
- Configurar los switch de forma básica.
- Configurar la dirección ip del pc.

Parte 3: Verificar y probar la conectividad de la red.

- Ver la configuración actual.
- Probar la conectividad con el comando ping.
- Probar las capacidades remotas mediante Telnet.
- Guardar el archivo de configuración del switch.

Parte 4: Gestionar la tabla de direcciones MAC.

- Guardar la dirección MAC del host.
- Determinar qué dirección MAC ha aprendido el switch.
- Mostrar las opciones de comandos en base al comando show mac address-table.
- Establecer una dirección estática MAC.

Imagen Original	Imagen Nueva
	
Se ha cambiado la interfaz usada por el switch.	
En este ejercicio se introducen nuevos conceptos como la conexión mediante consola entre PC y Switch. Además de las posibilidades remotas mediante Telnet, y la tabla de direcciones MAC.	

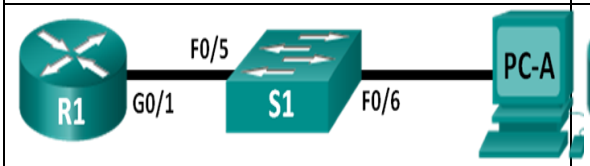
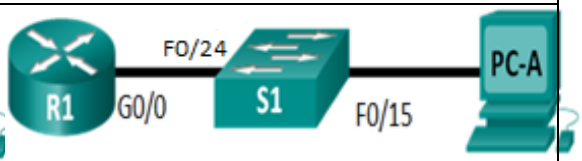
- Ejercicio 2.2.4.11 Configuración de características de seguridad de switch.

Objetivos:
Parte 1: Preparar la topología e inicializar los equipos.
Parte 2: Realizar las configuraciones básicas de los equipos y verificar su conectividad.
Parte 3: Configurar y verificar el acceso SSH en S1.

- Configurar el acceso SSH.
- Modificar los parámetros SSH.
- Verificar la configuración SSH.

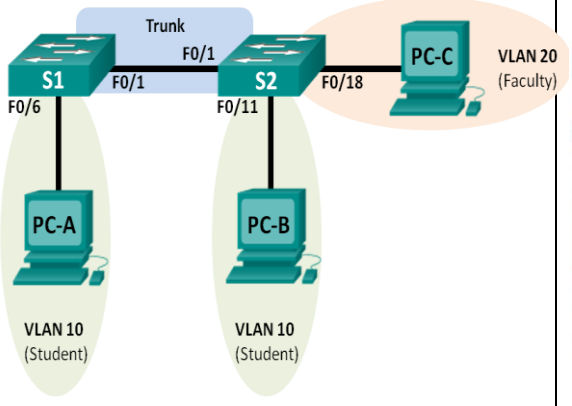
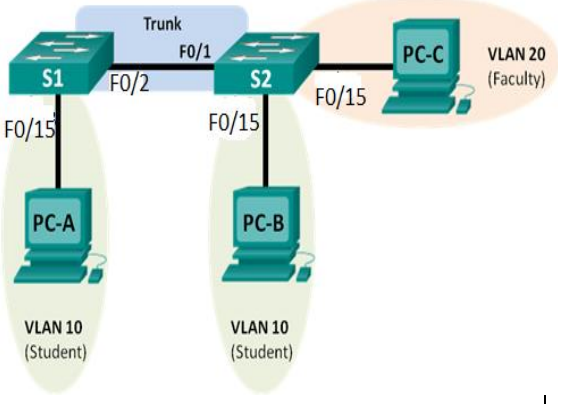
Parte 4: Configurar y verificar la seguridad en S1.

- Configurar y verificar los generales aspectos de seguridad.
- Configure y verificar la seguridad de puertos.

Imagen Original	Imagen Nueva
	
Se han cambiado todas las interfaces.	
Este ejercicio introduce nuevos conceptos como las conexiones remotas mediante SSH y los aspectos generales de seguridad de los switches.	

- Ejercicio 3.2.2.5 Configuración de redes VLAN y enlaces troncales.

Objetivos:
Parte 1: Construir la red y establecer las configuraciones básicas de los equipos de la red.
Parte 2: Crear VLANs y asignar los puertos del switch.
Parte 3: Mantener las asignaciones de los puertos para las VLAN y la base de datos de las VLAN.
Parte 4: Configure un enlace 802.1Q troncal entre los dos Switches.
Parte 5: Borrar la base de datos de VLAN.

Imagen Original	Imagen Nueva
	
Se han cambiado algunas interfaces. Las VLANs se dejan como estaban.	
Este ejercicio muestra por primera vez las VLANs dentro de una topología, sus respectivas asignaciones a diferentes puertos y los enlaces troncales entre switches.	

- Ejercicio 4.1.4.6 Configuración de los parámetros básicos de un router.

Objetivos:
Parte 1: Preparar la topología e inicializar los equipos.

- Preparar el cableado de la topología.
- Inicializar y reiniciar el router y el switch.

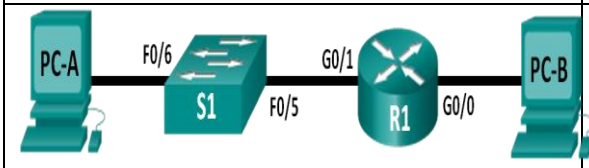
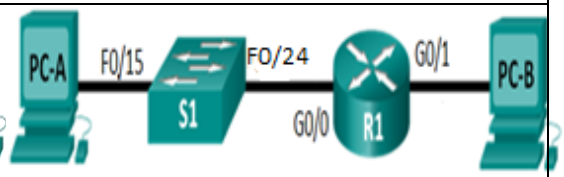
Parte 2: Configurar los equipos y verificar su conectividad.

- Asignar una IPv4 estática a las interfaces del PC.
- Configurar los parámetros básicos del router.
- Verificar la conectividad.
- Configurar el router por SSH.

Parte 3: Mostrar información del router.

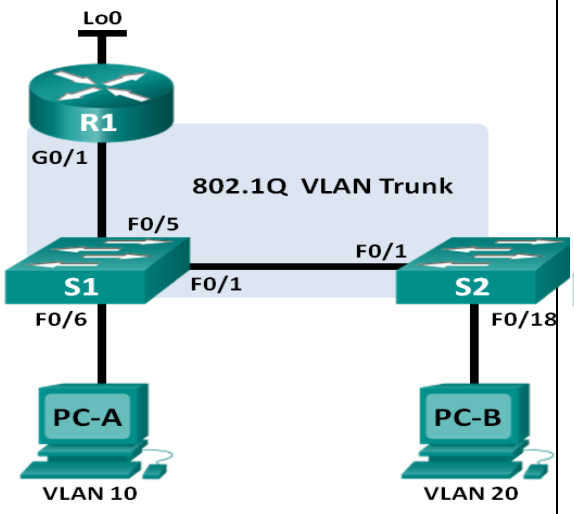
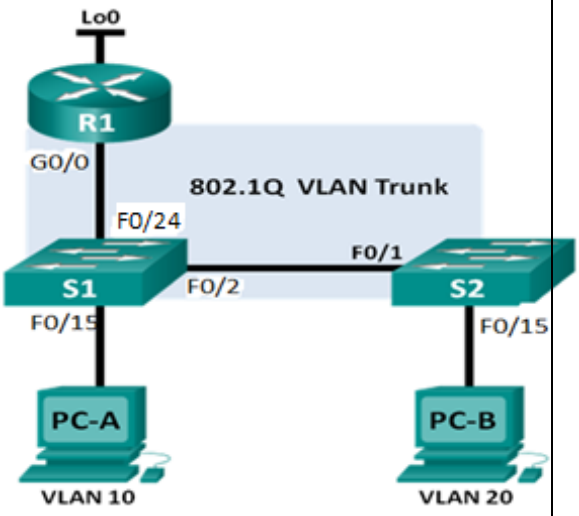
- Recopilar información del hardware y del software del router.
- Interpretar la salida del archivo startup de configuración.
- Interpretar la salida de la tabla de rutas.
- Verificar el estado de las interfaces.

Parte 4: Configurar y verificar la conectividad IPv6.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Además de repasar conceptos básicos de configuración y de SSH, se aprecia por primera vez IPv6.	

- Ejercicio 5.1.3.7 Configuración de routing entre VLAN basado en enlaces troncales 802.1Q.

Objetivos:
Parte 1: Construir la red y configurar de forma básica los equipos.
Parte 2: Configurar los Switches con VLANs y enlaces troncales.
Parte 3: Configurar los enlaces troncales de las VLANs entre los switches.

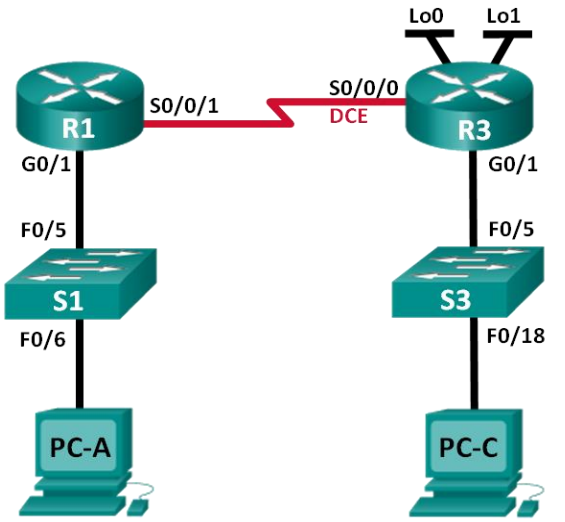
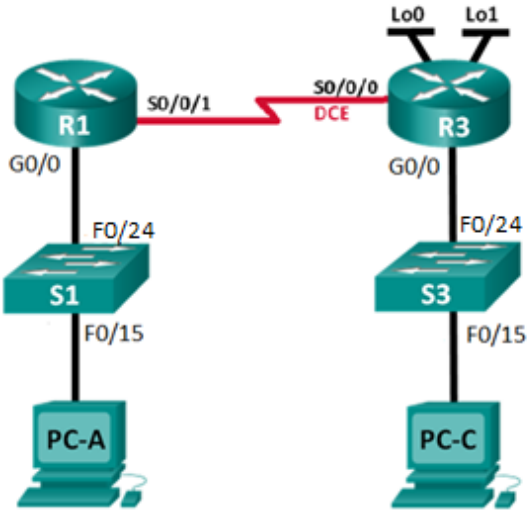
Imagen Original	Imagen Nueva
	
Se han modificado algunas interfaces, las VLANs y loopback se mantienen.	
Otro ejercicio que sirve para repasar la configuración de las VLANs y entre diferentes equipos.	

- Ejercicio 6.2.2.5 Configuración de rutas estáticas y predeterminadas IPv4.

Objetivos:
Parte 1: Preparar la topología e inicializar los equipos.
Parte 2: Configurar los equipos de forma básica y verificar su conectividad.
Parte 3: Configurar las rutas estáticas.

- Configurar una ruta recursiva estática.
- Configurar una ruta estática directamente conectada.
- Configurar y borrarlas rutas estáticas.

Parte 4: Configurar y verificar una ruta por defecto.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio explica cómo establecer rutas estáticas entres los dos routers.	

- Ejercicio 7.3.2.4 Configuración básica de RIPv2 y RIPng.

Objetivos:

Parte 1: Preparar la topología e inicializar los equipos.

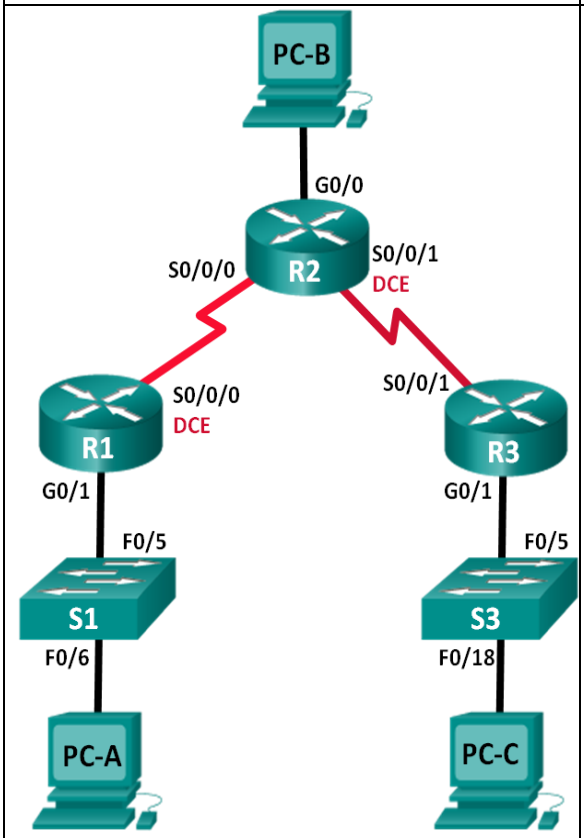
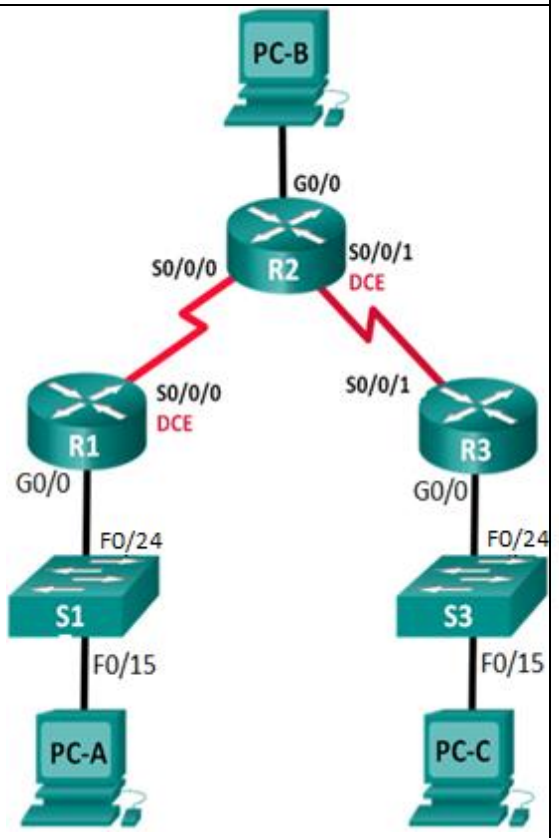
Parte 2: Configurar y verificar RIPv2.

- Configurar y verificar RIPv2 está funcionando en los routers.
- Configurar una interfaz pasiva.
- Examinar las tablas de rutas.
- Desactivar la sumarización automática.
- Configure una ruta por defecto.
- Verificar la conectividad.

Parte 3: Configurar IPv6 en los equipos.

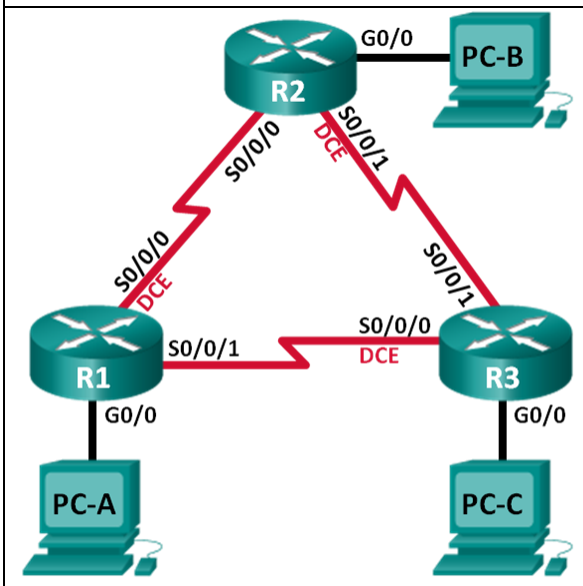
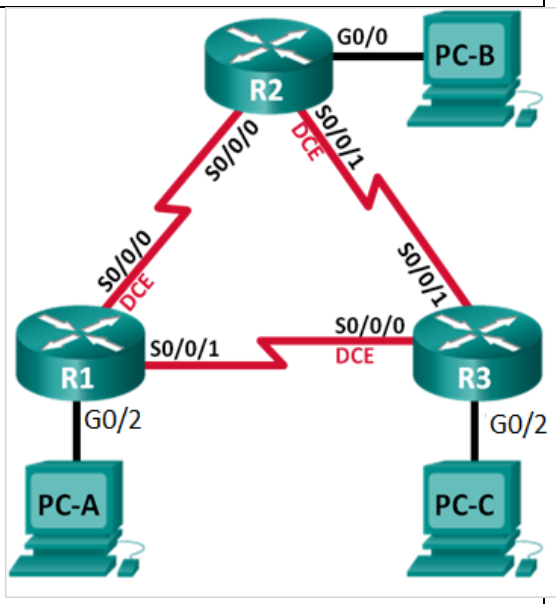
Parte 4: Configurar y verificar las rutas RIPng.

- Configure y verificar que RIPng está funcionando en los routers.
- Examinar las tablas de rutas.
- Configurar una ruta por defecto.
- Verificar la conectividad.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Por primera vez, los alumnos podrán utilizar el protocolo RIPv2 de encaminamiento. Es un protocolo de puerta de enlace interna o IGP (Interior Gateway Protocol) utilizado por los routers (encaminadores) para intercambiar información acerca de redes IP a las que se encuentran conectados. Su algoritmo de encaminamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable.	

- Ejercicio 8.2.4.5 Configuración de OSPFv2 básico de área única.

Objetivos:
Parte 1: Construir la red y la configuración básica de los equipos.
Parte 2: Configurar y verificar las rutas de OSPF.
Parte 3: Cambiar la asignación del ID del Router.
Parte 4: Configurar las interfaces pasivas de OSPF.
Parte 5: Cambiar la métrica de OSPF.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
En este ejercicio se estudia por primera vez el protocolo de encaminamiento OSPF, estas son las siglas de Open Shortest Path First (El camino más corto primero), un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo SmoothWall Dijkstra enlace-estado (LSE - Link State Algorithm) para calcular la ruta más idónea. Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.	

- Ejercicio 9.2.2.7 Configuración y verificación de ACL estándares.

Objetivos:

Parte 1: Preparar la topología e inicializar los equipos.

- Preparar el equipamiento para albergar la topología.
- Inicializar y recargar la configuración de routers y switches.

Parte 2: Configurar los equipos y verificar su conectividad.

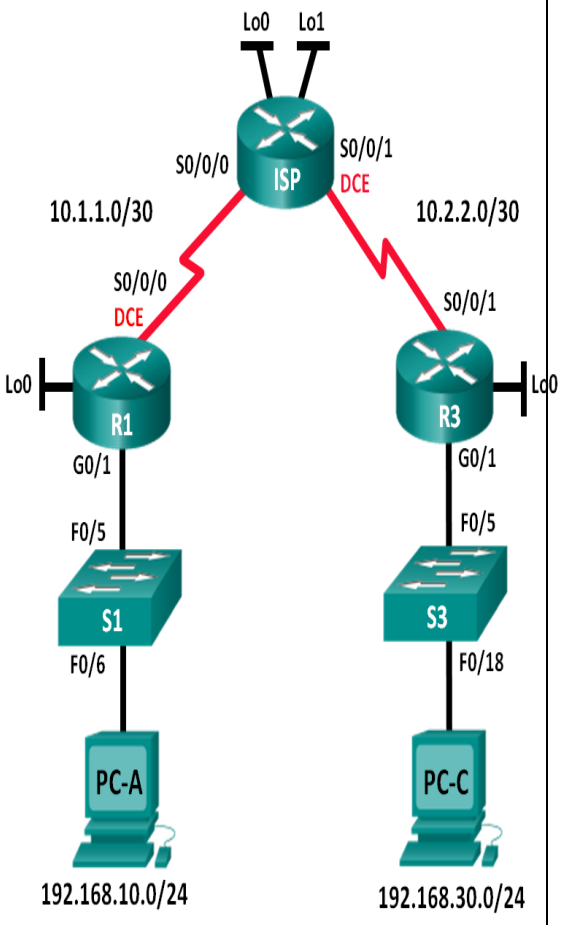
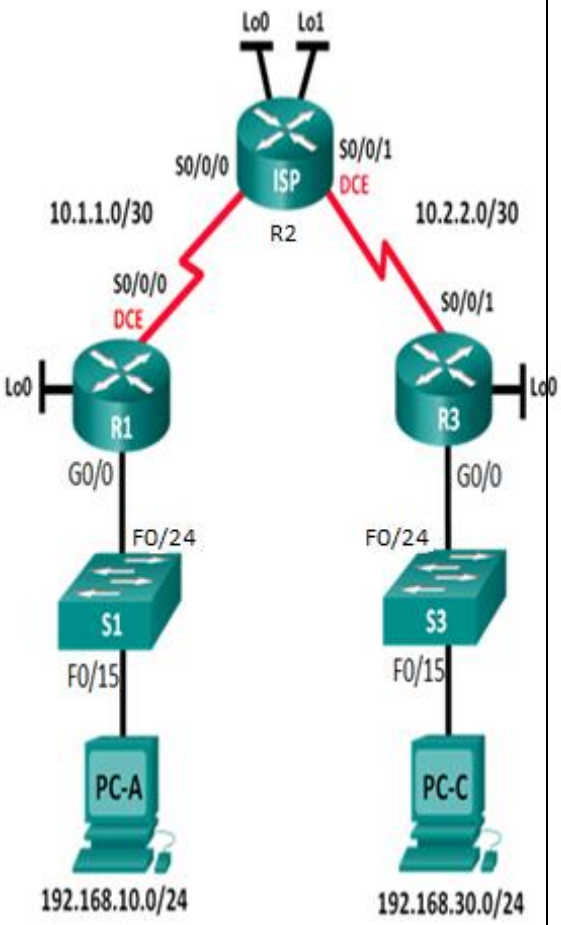
- Asignar una dirección IP estática a los PCs.
- Configurar los parámetros básicos en los routers.
- Configurar los parámetros básicos en los switches.
- Configurar OSPF en R1, ISP, y R3.
- Verificar la conectividad entre los equipos.

Parte 3: Configurar y verificar las ACLs nombradas y las estándar numeradas.

- Configurar, aplicar y verificar una ACL estándar numerada.
- Configurar, aplicar y verificar una ACL nombrada.

Parte 4: Modificar una ACL estándar.

- Modificar y verificar una ACL estándar nombrada.
- Probar la ACL.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio, además de reforzar lo visto sobre OSPF, sirve como toma de contacto de las ACL. Un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. En este caso se utilizan las direcciones ip origen y destino para restringir su paso.	

- Ejercicio 9.3.2.13 Configuración y verificación de ACL extendidas.

Objetivos:

Parte 1: Preparar la topología e inicializar los equipos.

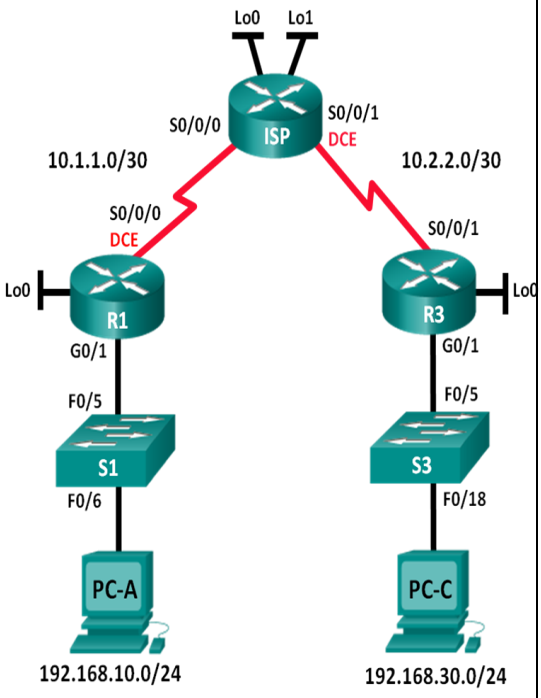
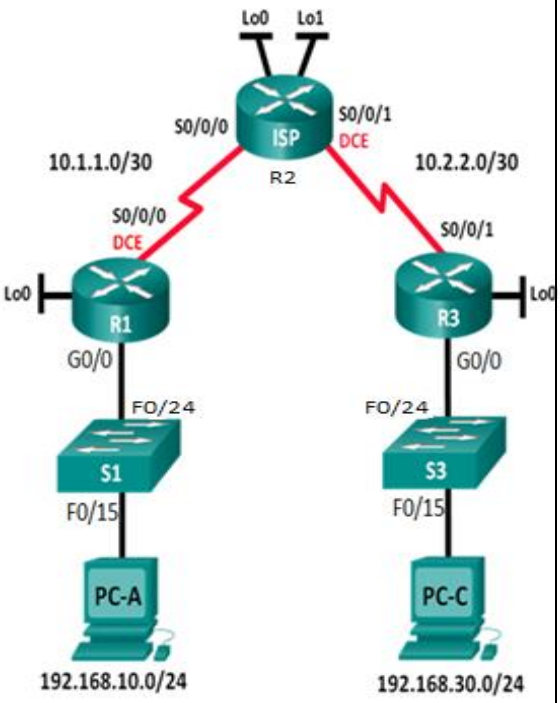
Parte 2: Configurar los equipos y verificar la conectividad.

- Configuración básica de PCs, routers, y switches.
- Configurar OSPF en R1, ISP, y R3.

Parte 3: Configurar y verificar las ACLs nombradas y las extendidas numeradas.

- Configurar, aplicar y verificar una ACL extendida numerada.
- Configurar, aplicar y verificar una ACL extendida nombrada.

Parte 4: Modificar y verificar las ACLs extendidas.

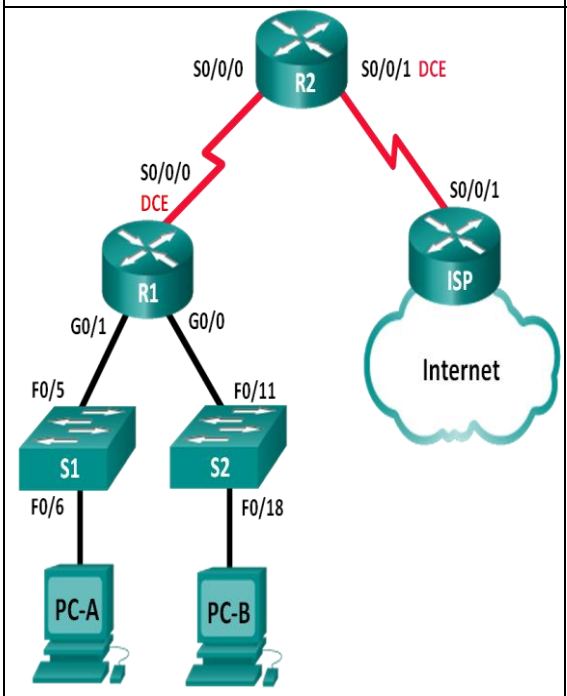
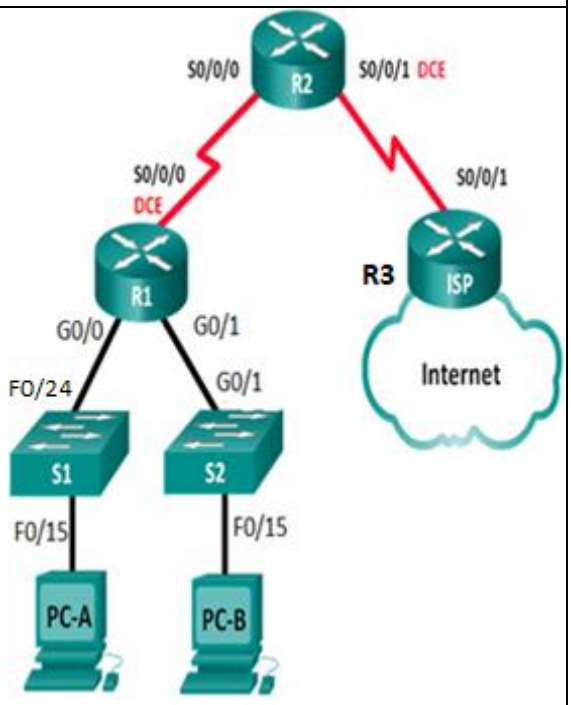
Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio continúa repasando conceptos como OSPF y las ACLs. En esta ocasión añade las ACL extendidas, mucho más complejas de realizar, pudiendo filtrar por protocolos y equipos.	

- Ejercicio: 10.1.2.4 Configuración de DHCPv4 básico en un router.

Objetivos:

Parte 1: Construir la red y realizar la configuración básica de los equipos.

Parte 2: Configurar un servidor DHCPv4 Server y un agente Relay DHCP.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces. El ISP pasa a ser R3.	
Ejercicio de importancia al introducir por primera vez el protocolo dinámico DHCP, en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.	

5.2.3 MÓDULO 3, “SCALLING NETWORKS”

- Ejercicio 2.3.2.3 Configuración de PVST+ rápido, PortFast y protección BPDU.

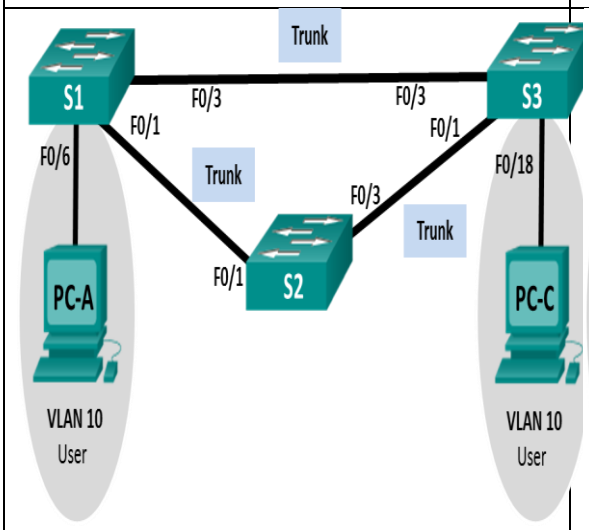
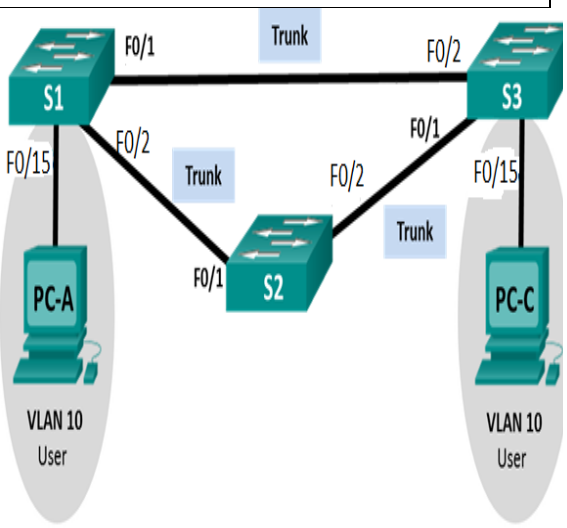
Objetivos:

Parte 1: Construir la red y realizar la configuración básica de los equipos.

Parte 2: Configurar las VLANs, VLAN nativas, y troncales.

Parte 3: Configurar el puente raíz y examinar la convergencia PVST+.

Parte 4: Configurar Rapid PVST+, PortFast, y examinar la convergencia.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces. Las VLANs se mantienen.	
Este ejercicio continúa repasando conceptos como las VLANs, y además introduce por primera vez aspectos de la convergencia de la red, portfast y dispositivos que actúan como puente raíz.	

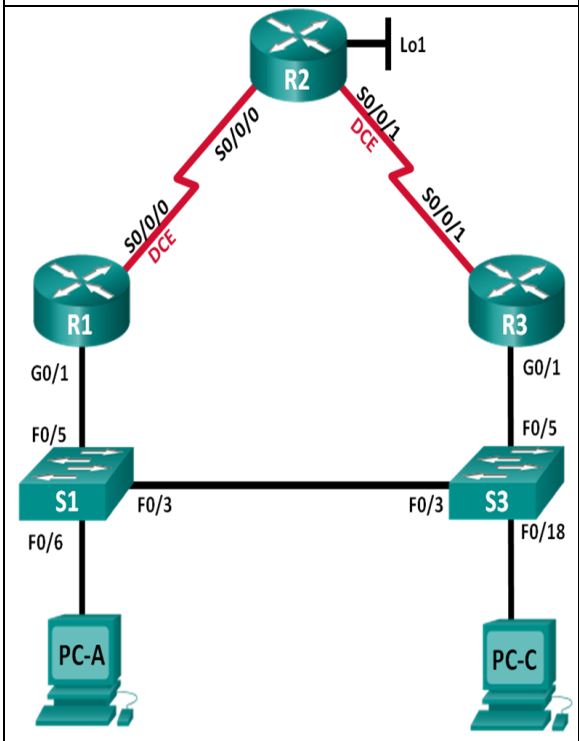
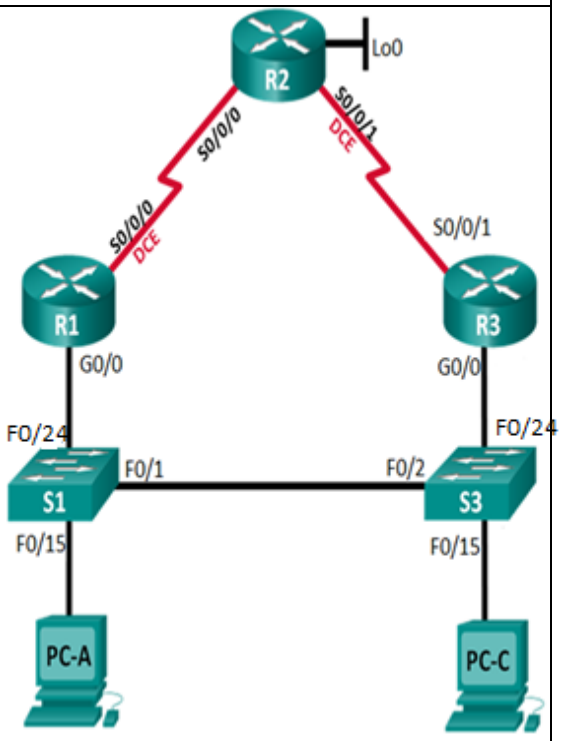
- Ejercicio 2.4.3.4 Configuración de HSRP y GLBP.

Objetivos:

Parte 1: Construir la red y verificar la conectividad.

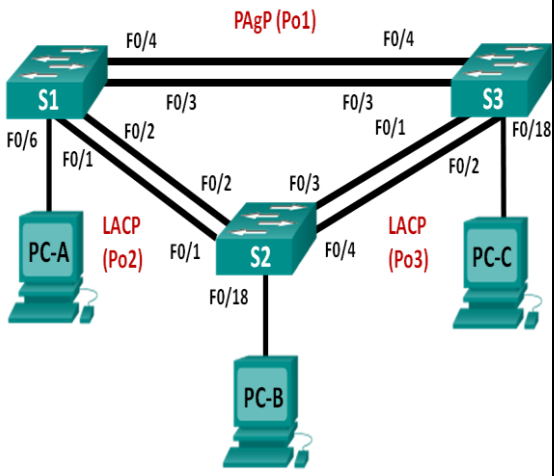
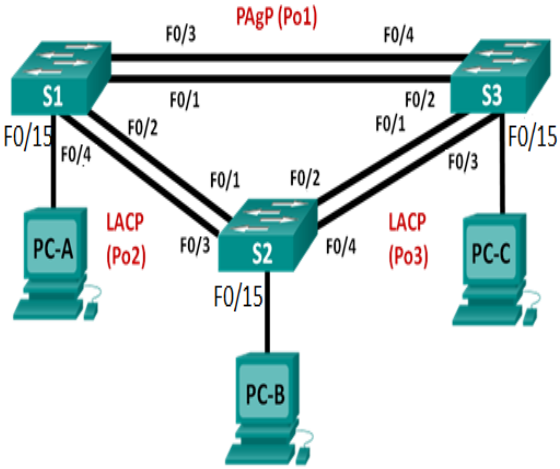
Parte 2: Configurar el primer salto usando HSRP para la redundancia.

Parte 3: Configurar el primer salto usando GLBP para la redundancia.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio introduce nuevos protocolos de redundancia como HSRP y GLBP. El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Gateway Protocol Load Balancing (GLBP) es un protocolo propiedad de CISCO que intenta superar las limitaciones de los protocolos de router redundantes existentes añadiendo una funcionalidad básica de balanceo de carga.	

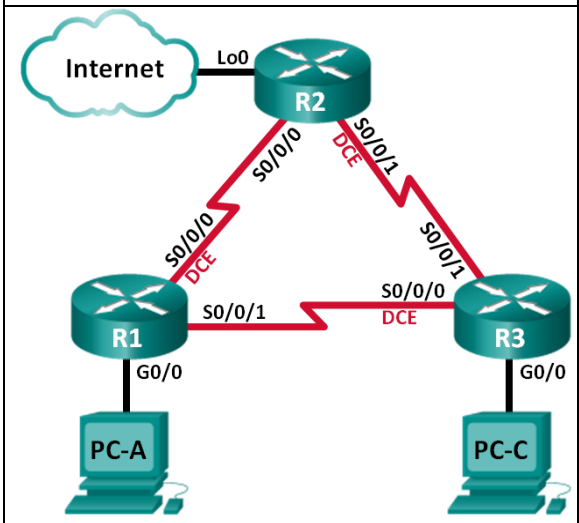
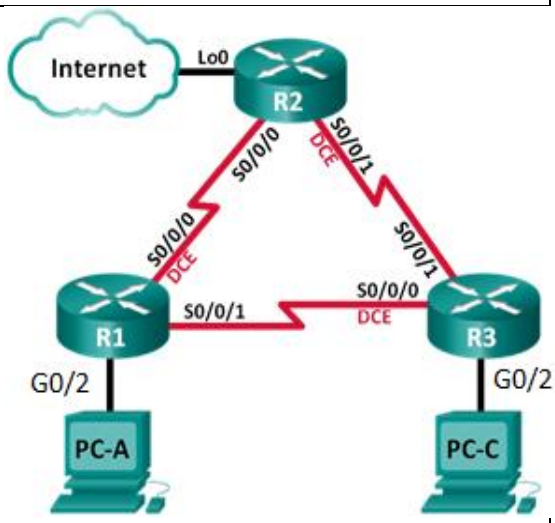
- Ejercicio 3.2.1.4 Configuración de EtherChannel.

Objetivos:
Parte 1: Configuración básica de los Switches.
Parte 2: Configurar PAgP.
Parte 3: Configurar LACP.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio introduce el concepto de Etherchannel y alguno de sus protocolos. Protocolo Port Aggregation (PAgP) es un protocolo propiedad de Cisco, que se utiliza para el automatizado, la agregación lógica de puertos Ethernet de conmutación, conocidos como etherchannel. El switch negocia con el otro extremo cuales son los puertos que deben ponerse activos. El propio protocolo se encarga de agrupar puertos con características similares. Link Aggregation Control Protocol (LACP) es muy similar a PAgP ya que también puede agrupar puertos con características similares.	

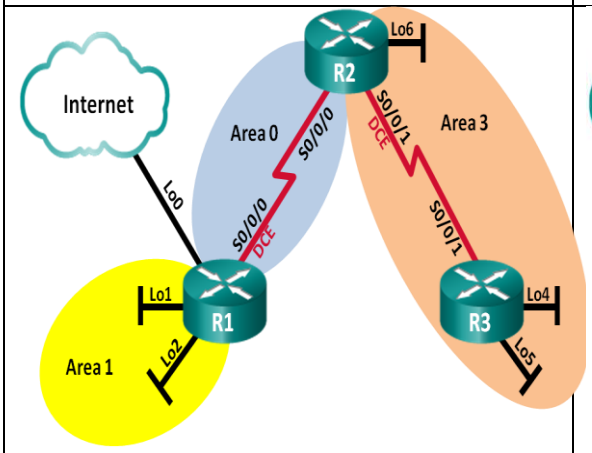
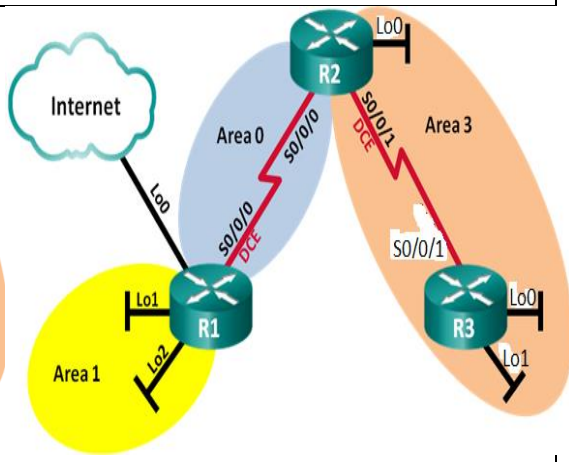
- Ejercicio 5.1.5.8 Configuración de las características avanzadas de OSPFv2.

Objetivos:
Parte 1: Construir la red y configurar los equipos de forma básica.
Parte 2: Configurar y verificar OSPF.
Parte 3: Cambiar las métricas de OSPF.
Parte 4: Configurar y propagar una ruta estática por defecto.
Parte 5: Configurar la autenticación OSPF.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio permite ver más características del protocolo de encaminamiento OSPF.	

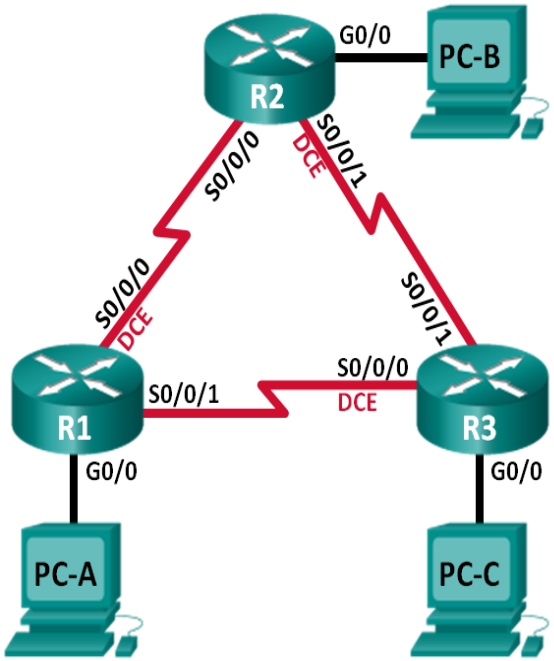
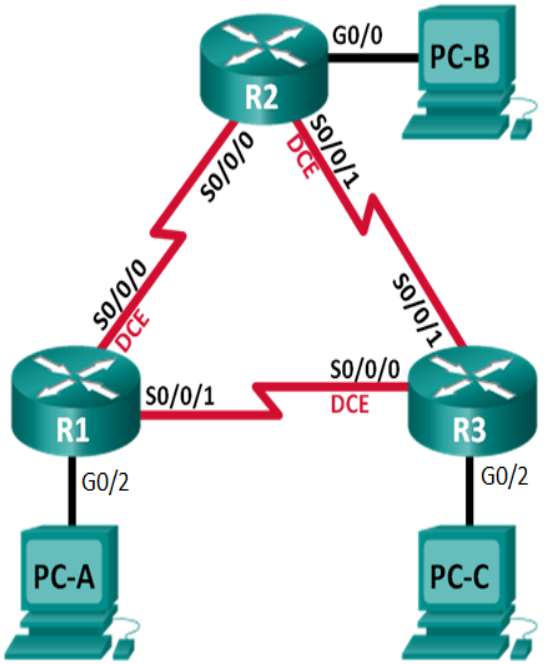
- Ejercicio 6.2.3.8 Configuración de OSPFv2 multiárea.

Objetivos:
Parte 1: Construir la red y configurar de forma básica los equipos.
Parte 2: Configurar una red multiárea OSPFv2.
Parte 3: Configurar rutas sumarizadas a las áreas.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces. Las áreas se mantienen.	
Este ejercicio continúa explicando más conceptos sobre el protocolo de encaminamiento OSPFv2. En esta ocasión presentando diferentes áreas.	

- Ejercicio 7.2.2.5 Configuración de EIGRP básico para IPv4.

Objetivos:
Parte 1: Construir la red y verificar la conectividad.
Parte 2: Configurar EIGRP Routing.
Parte 3: Verificar EIGRP Routing.
Parte 4: Configurar el ancho de banda (Bandwidth) y las interfaces pasivas.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Por primera vez se introduce otro protocolo de encaminamiento, EIGRP. es un protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.	

- Ejercicio 8.1.5.5 Configuración de EIGRP avanzado para admitir características de IPv4.

Objetivos:

Parte 1: Construir la red y realizar la configuración básica de los equipos.

Parte 2: Configure EIGRP y verificar la conectividad.

Parte 3: Configurar la sumarización para EIGRP.

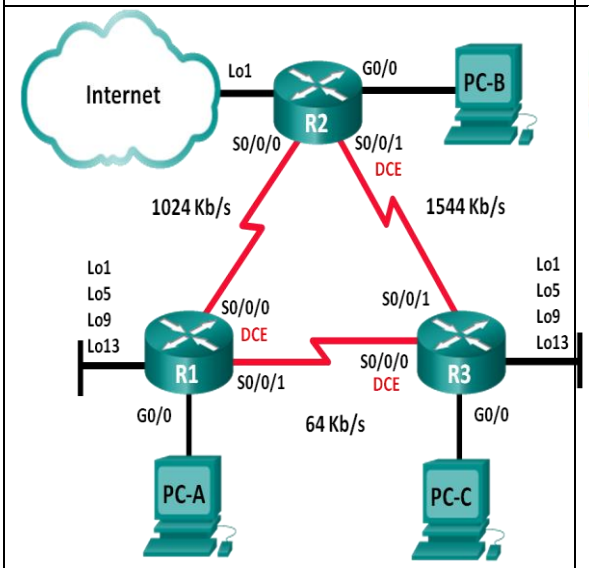
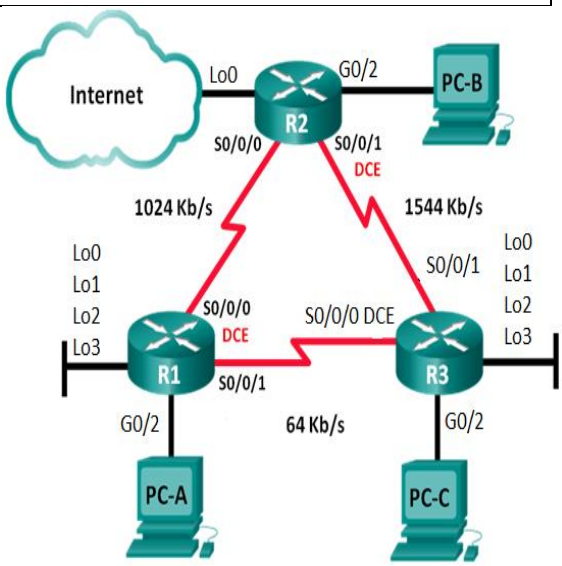
- Configurar la automática sumarización para EIGRP.
- Configurar la manual sumarización para EIGRP.

Parte 4: Configurar y propagar una ruta estática por defecto.

Parte 5: Ajustar EIGRP.

- Configurar el ancho de banda para EIGRP.
- Configurar los diferentes intervalos y tiempos para EIGRP.

Parte 6: Configurar la autenticación EIGRP.

<table>
<tr><th>Imagen Original</th><th>Imagen Nueva</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td colspan="2">Se han modificado las interfaces.</td></tr>
<tr><td colspan="2">Se sigue utilizando el protocolo EIGRP pero con un mayor número de opciones.</td></tr>
</table>

5.2.4 MÓDULO 4, “CONNECTING NETWORKS”

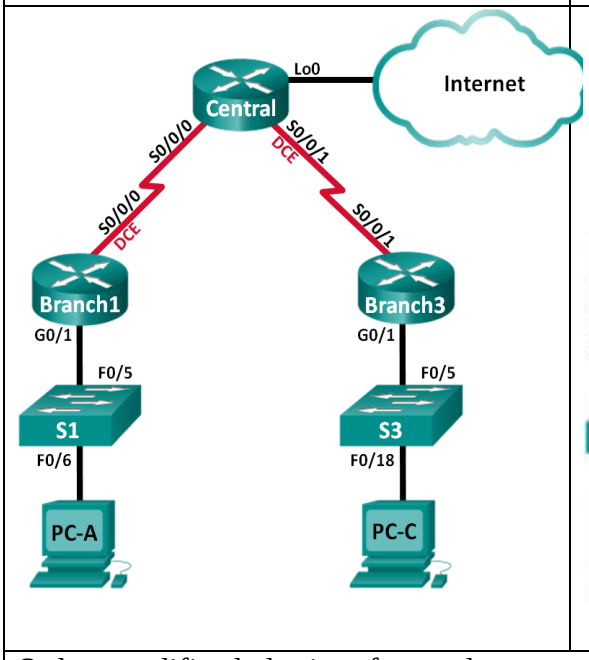
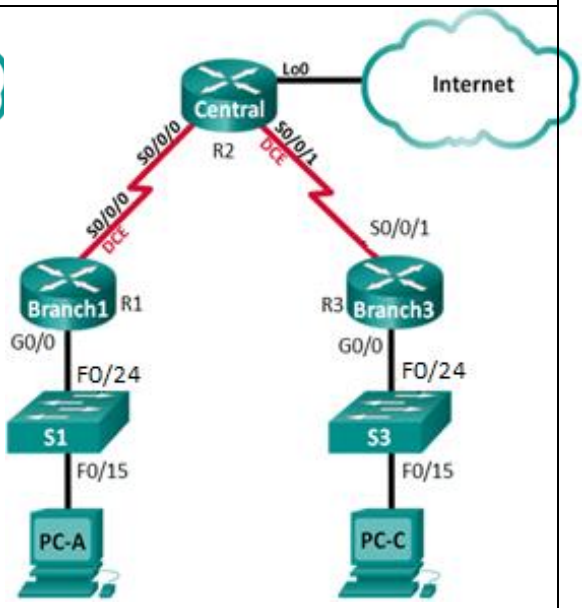
- Ejercicio 3.3.2.8 Configuración de PPP básico con autenticación.

Objetivos:

Parte 1: Configuración básica de los equipos.

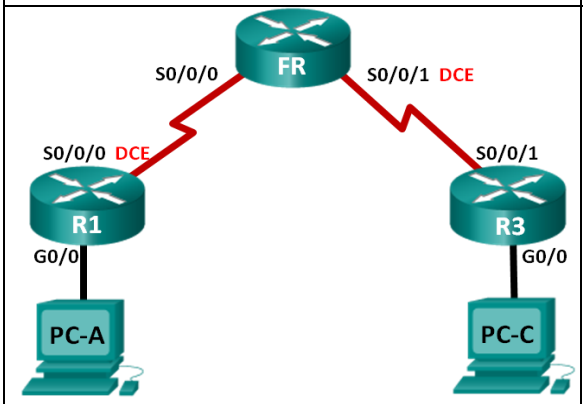
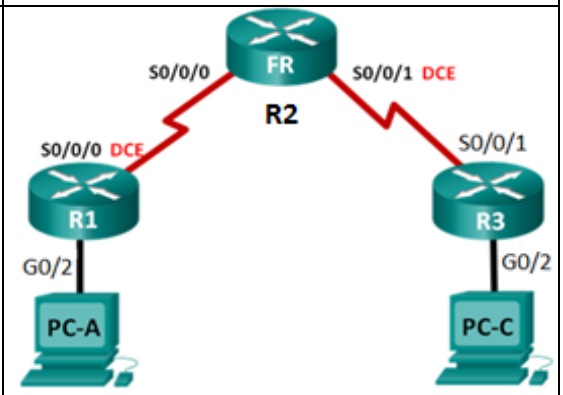
Parte 2: Configurar encapsulación PPP.

Parte 3: Configurar autenticación PPP CHAP.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces y la nomenclatura de los routers.	
Este ejercicio introduce a los alumnos un nuevo protocolo, PPP. Point-to-point Protocol (en español Protocolo punto a punto), también conocido por su acrónimo PPP, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Comúnmente usado para establecer una conexión directa entre dos nodos de red.	

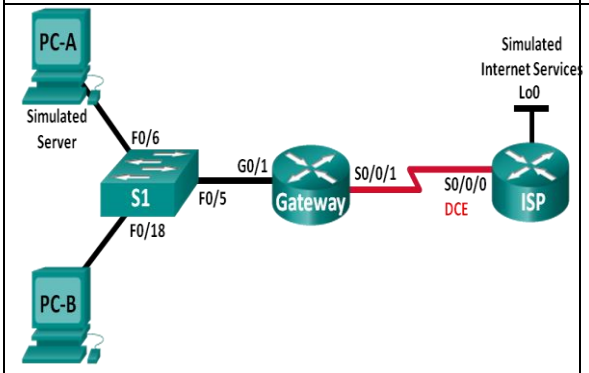
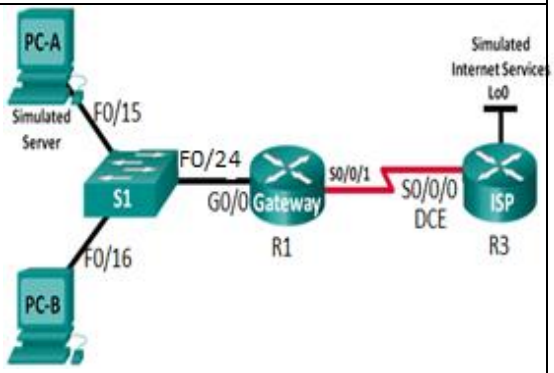
- Ejercicio 4.2.2.7 Configuración de Frame Relay y subinterfaces.

Objetivos:
Parte 1: Construir la red y la configuración básica de los equipos.
Parte 2: Configurar Frame Relay Switch.
Parte 3: Configuración básica de Frame Relay.
Parte 4: Probar Frame Relay.
Parte 5: Configure una subinterfaz de Frame Relay.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio introduce la técnica de Frame Relay. Frame Relay o (Frame-mode Bearer Service) es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducido por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos. La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor.	

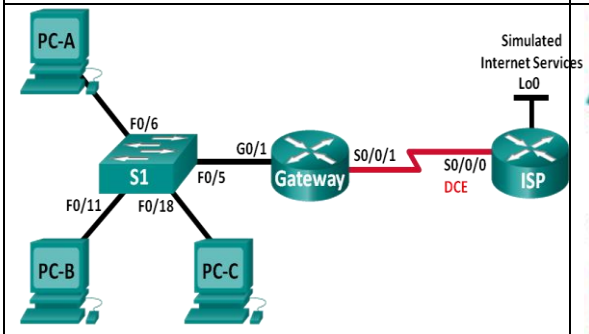
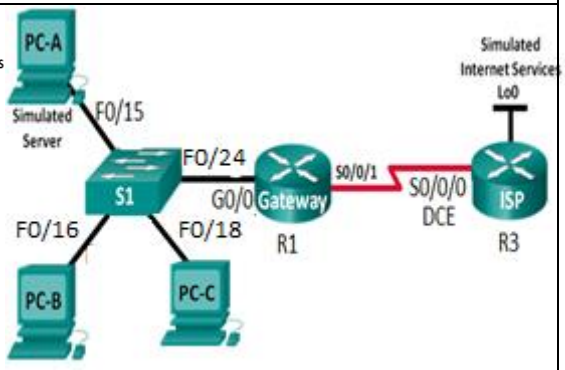
- Ejercicio 5.2.2.6 Configuración de NAT dinámica y estática.

Objetivos:
Parte 1: Construir la red y verificar la conectividad.
Parte 2: Configurar y verificar la NAT estática.
Parte 3: Configurar y verificar la NAT dinámica.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces y el nombrado de los Routers.	
Un nuevo concepto, la NAT, es introducido en este ejercicio. NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados.	

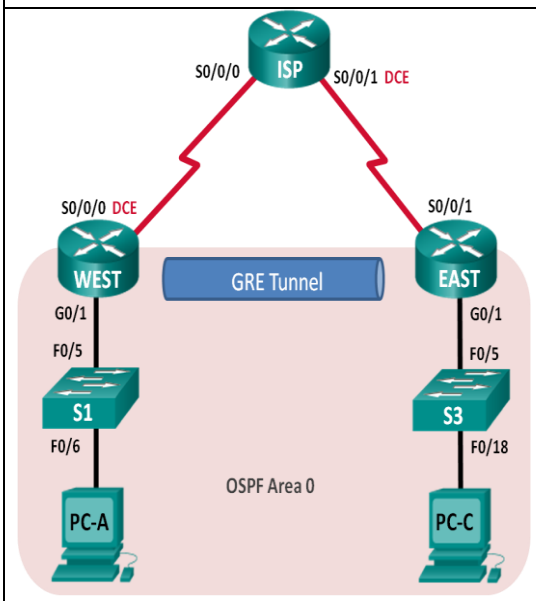
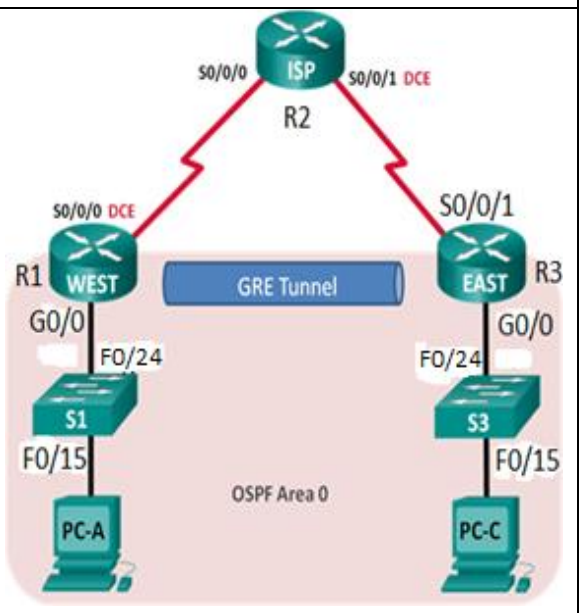
- Ejercicio 5.2.3.7 Configuración de la traducción de la dirección del puerto (PAT).

Objetivos:
Parte 1: Construir la red y verificar la conectividad.
Parte 2: Configurar y verificar el pool NAT con sobrecarga (NAT Pool Overload)
Parte 3: Configurar y verificar PAT.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces y el nombrado de los Routers.	
En este ejercicio se ven más opciones sobre NAT, como la sobrecarga y los pools, además de PAT. Port Address Translation (PAT) es una característica del estándar NAT, que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. Permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a ~64000 direcciones internas.	

- Ejercicio 7.2.2.5 Configuración de un túnel VPN GRE de punto a punto.

Objetivos:
Parte 1: Configuración básica de los equipos.
Parte 2: Configurar un GRE Tunnel.
Parte 3: Activar el tráfico en el GRE Tunnel.

<table>
<tr><th>Imagen Original</th><th>Imagen Nueva</th></tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr><td colspan="2">Se han modificado las interfaces y el nombrado de los Routers.</td></tr>
<tr><td colspan="2">El ejercicio muestra como configurar un GRE Tunnel. El GRE (Generic Routing Encapsulation) es un protocolo para el establecimiento de túneles a través de Internet. Desarrollado por Cisco Systems puede encapsular una amplia variedad de protocolos dentro enlaces punto a punto virtuales.</td></tr>
</table>

5.2.5 CCNA SECURITY:

- Ejercicio 2.5.1.1 Securización del router para acceso administrativo.

Objetivos:

Parte 1: Configuración básica de los equipos.

- Realizar el cableado según muestra la topología.
- Configuración básica del direccionamiento IP para routers y PCs.
- Configurar rutas estáticas, incluidas las por defecto.
- Verificar la conectividad entre los hosts y los routers.

Parte 2: Acceso de control administrativo para los routers.

- Configurar y encriptar todas las contraseñas.
- Configurar un mensaje de peligro de login.
- Configurar contraseña de seguridad de nombre de usuario mejorada.
- Configurar seguridad virtual del login mejorada.
- Configurar un servidor SSH en el router.
- Configurar un cliente SSH y verificar la conectividad.

Parte 3: Configurar roles administrativos.

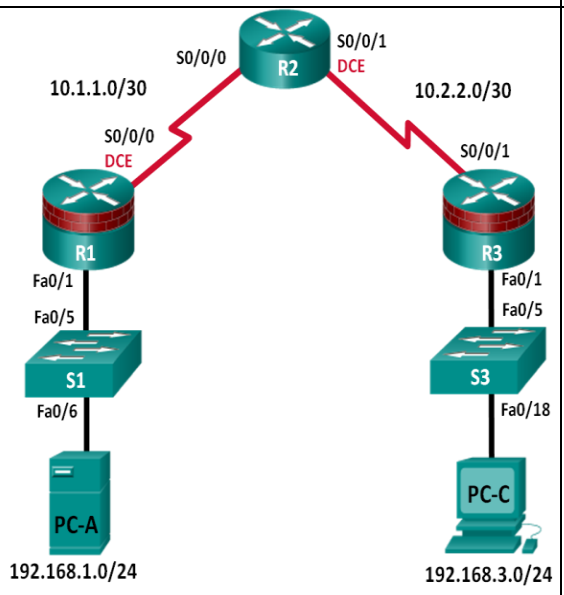
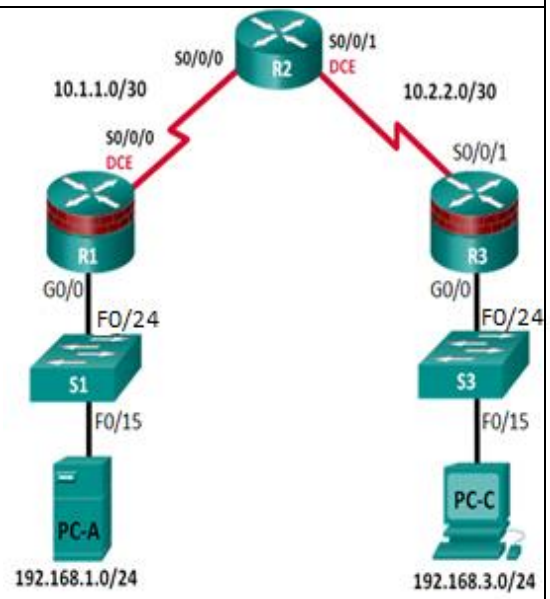
- Crear múltiples vistas de roles y ver sus privilegios.
- Verificar y contrastar las vistas.

Parte 4: Configurar Cisco IOS y la gestión de la información.

- Asegurar la imagen de Cisco IOS y los archivos de configuración.
- Configurar un router como fuente sincronizada para otros equipos que usen NTP.
- Configurar un Syslog en el router.
- Instalar un servidor Syslog server en un PC y activarlo.
- Configurar reportes en el router usando SNMP.
- Hacer cambios en el router y ver los resultados en el PC mediante el Syslog.

Parte 5: Configurar características automáticas de seguridad

- Usar AutoSecure en el router y verificar la configuración.
- Usar la herramienta de seguridad CCP Security Audit tool para identificar vulnerabilidades y bloquear servicios.
- Contrastar la configuración de autoseguridad con CCP.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio incorporar los primeros conceptos sobre seguridad dentro de una topología. Desde los más básicos como las contraseñas o las líneas SSH hasta otros más complejos capaces de observar posibles vulnerabilidades desde programas externos.	

- Ejercicio 3.6.1.1 Securización de acceso administrativo usando AAA y servidor Radius.

Objetivos:

Parte 1: Configuración básica de los equipos.

- Configuración básica como el host name, direcciones IP de interfaces y contraseñas de acceso.
- Configurar rutas estáticas.

Parte 2: Configurar autenticación local.

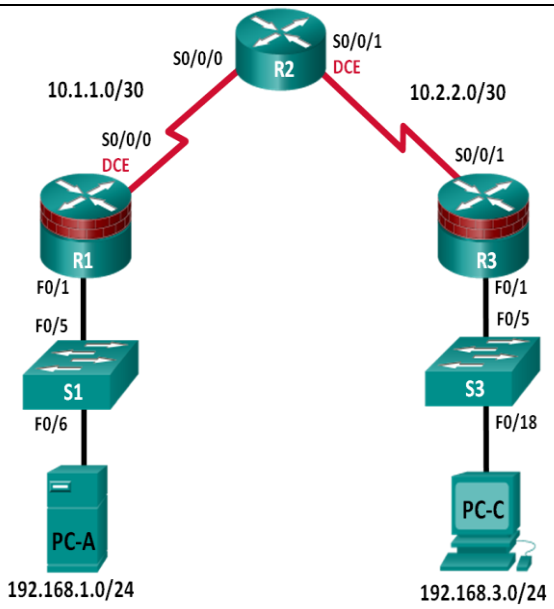
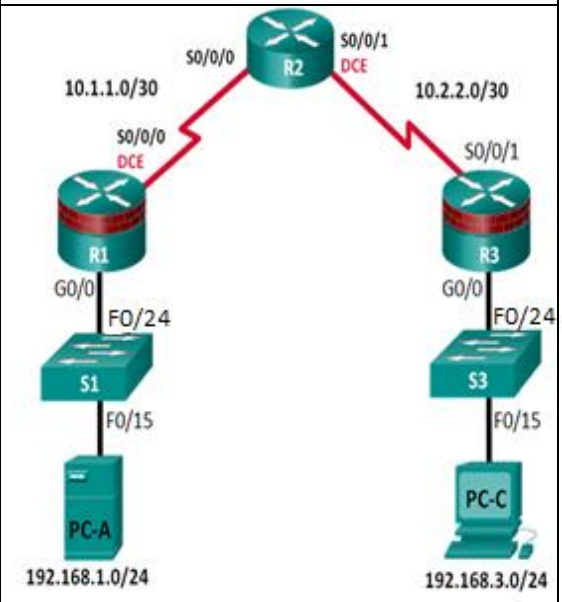
- Configurar una base de datos local de usuarios y accesos locales por consola, vty y líneas auxiliares.
- Probar la configuración.

Parte 3: Configurar autenticación local usando AAA.

- Configurar la base de datos local de usuarios usando Cisco IOS.
- Configurar la autenticación AAA local usando Cisco IOS.
- Configure la autenticación AAA local usando CCP.
- Probar la configuración.

Parte 4: Configurar una autenticación centralizada usando AAA y RADIUS.

- Instalar un servidor RADIUS server en un ordenador.
- Configurar los usuarios en el servidor RADIUS.
- Usar Cisco IOS para configurar servicios AAA en un router para acceder al servidor RADIUS para autenticarse.
- Usar CCP para configurar servicios AAA en un router para acceder al servidor RADIUS para autenticarse.
- Probar la configuración AAA RADIUS.

<table>
<tr><th>Imagen Original</th><th>Imagen Nueva</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td colspan="2">Se han modificado las interfaces.</td></tr>
<tr><td colspan="2">Este ejercicio añade nuevas características a la hora de securizar los diferentes equipos, incluyendo AAA y servidor RADIUS. AAA es un marco arquitectónico para la configuración de un conjunto de tres funciones de seguridad independientes de una manera consistente. RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.</td></tr>
</table>

- Ejercicio 4.4.1.1 Configurar políticas zonales mediante Firewalls.

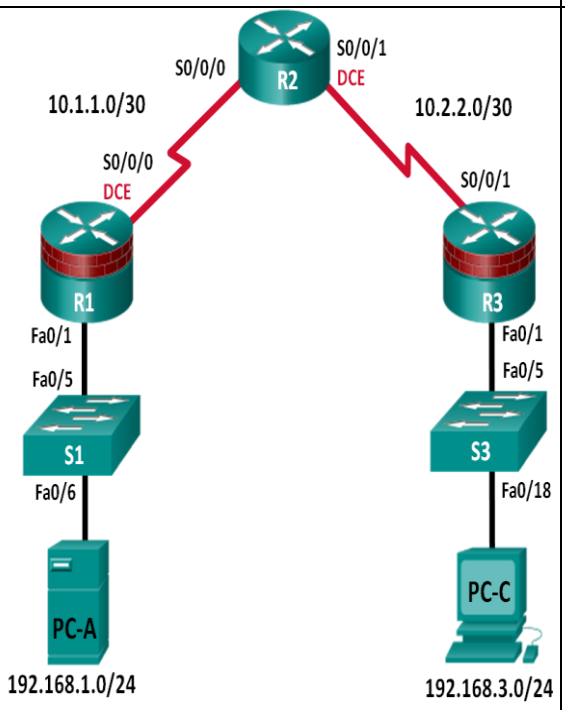
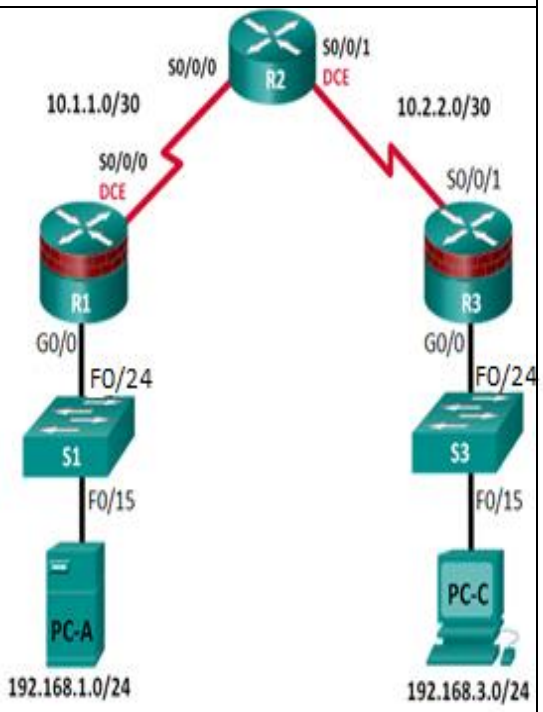
Objetivos:

Parte 1: Configuración básica del router.

- Configuración básica como el host name, direcciones IP de interfaces y contraseñas de acceso.
- Configurar OSPF.
- Usar el puerto Nmap para escanear vulnerabilidades del router.

Parte 2: Configurar políticas zonales mediante Firewalls (ZBF)

- Usar CCP para configurar ZBF.
- Usar CCP Monitor para verificar la configuración.

<table>
<tr><th>Imagen Original</th><th>Imagen Nueva</th></tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr><td colspan="2">Se han modificado las interfaces.</td></tr>
<tr><td colspan="2">Este ejercicio introduce el concepto ZBF. Es el método más avanzado en el que un firewall de estado que se encuentra disponible en los routers Cisco IOS. La idea detrás de ZBF es que nosotros no asignamos listas de acceso a las interfaces, pero vamos a crear diferentes zonas. Las interfaces serán asignadas a las diferentes zonas y las políticas de seguridad deben estar asignados a tráfico entre zonas.</td></tr>
</table>

- Ejercicio 5.5.1.1 Configurar un sistema de prevención de intrusiones (IPS) usando CLI y CCP.

Objetivos:

Parte 1: Configuración básica del router.

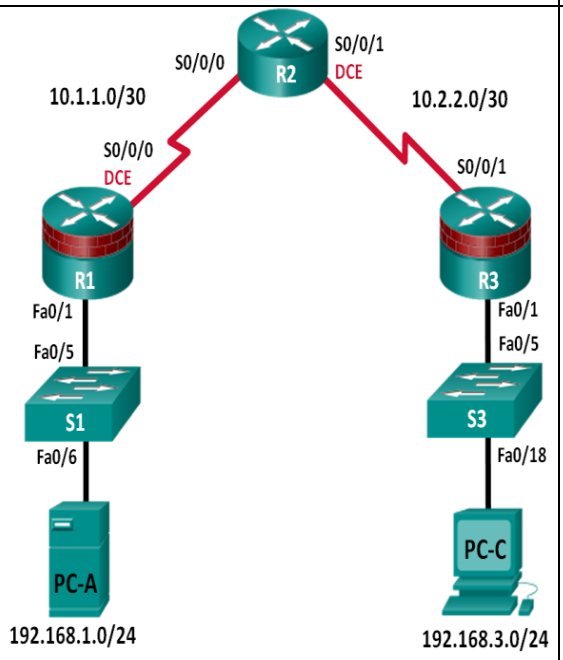
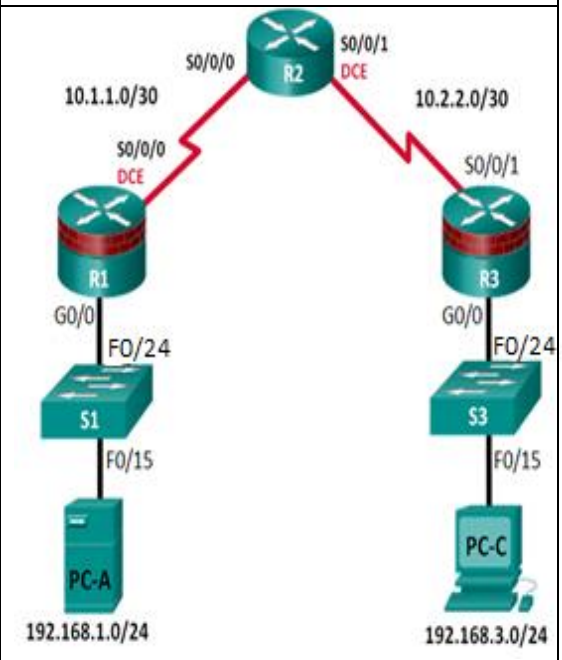
- Configuración básica como el host name, direcciones IP de interfaces y contraseñas de acceso.
- Configurar las rutas estáticas.

Parte 2: Usar CLI para configurar un IOS IPS.

- Configurar el IOS (IPS) usando CLI.
- Modificar las firmas de IPS.
- Examinar los resultados de la configuración IPS.
- Verificar la funcionalidad de IPS.
- Establecer mensajes IPS para servidor syslog.

Parte 3: Configurar IPS usando CCP.

- Configurar IPS usando CCP.
- Modificar las firmas de IPS.
- Examinar los resultados de la configuración IPS.
- Usar una herramienta de escáner en un ataque simulado.
- Usar CCP Monitor para verificar la funcionalidad de IPS.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	

Este ejercicio introduce el sistema de prevención de intrusiones (IPS) de Cisco. Un componente del marco de control de amenazas de Cisco IOS integrado que proporciona a la red la posibilidad de identificar con exactitud, clasificar y detener o bloquear el tráfico malicioso en tiempo real.

- Ejercicio 6.5.1.1 Asegurar la segunda capa de los switches.

Objetivos:

Parte 1: Configuración básica del switch.

- Construir la topología.
- Configuración básica como el host name, direcciones IP de interfaces y contraseñas de acceso.

Parte 2: Configurar acceso SSH a los switches.

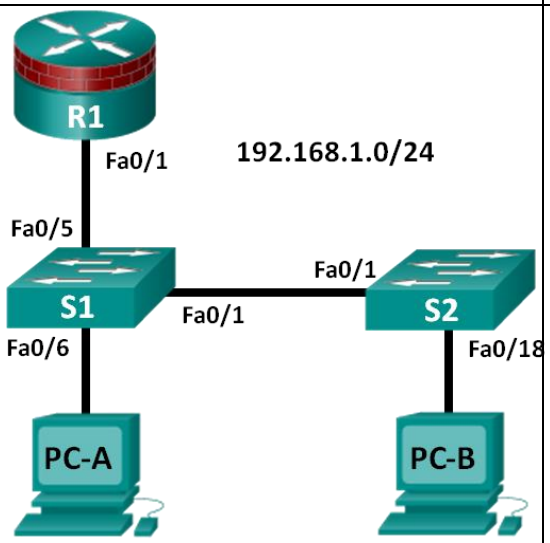
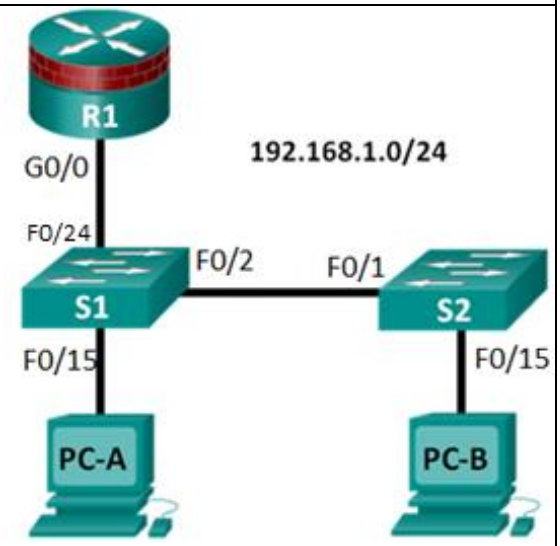
- Configurar acceso SSH en el switch.
- Configurar un cliente SSH para acceder al switch.
- Verificar la configuración.

Parte 3: Configurar la seguridad en troncales y puertos de acceso.

- Configurar modo troncal de puerto.
- Cambiar la VLAN nativa para los puertos troncales.
- Verificar la configuración troncal.
- Activar "storm control" para broadcasts.
- Configurar puertos de acceso.
- Activar PortFast y BPDU.
- Verificar BPDU.
- Activar root guard.
- Configurar y verificar la seguridad de los puertos.
- Desactivar puertos no usados.
- Mover los puertos de la VLAN 1 por defecto a una VLAN alternativa.
- Configurar PVLAN Edge en un puerto.

Parte 4: Configurar SPAN y monitorizar el tráfico.

- Configurar Switched Port Analyzer (SPAN).
- Monitorizar la actividad del puerto usando Wireshark.
- Analizar la fuente de un ataque.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio repasa conceptos de seguridad básicos ya vistos, pero se centra en la seguridad de los puertos de los switches y sus respectivas VLANs. Además introduce el programa de monitorización Wireshark, bastante utilizado en la asignatura.	

- Ejercicio 8.7.1.1 Configurar una Site-to-Site VPN usando Cisco IOS y CCP.

Objetivos:

Parte 1: Configuración básica de los equipos.

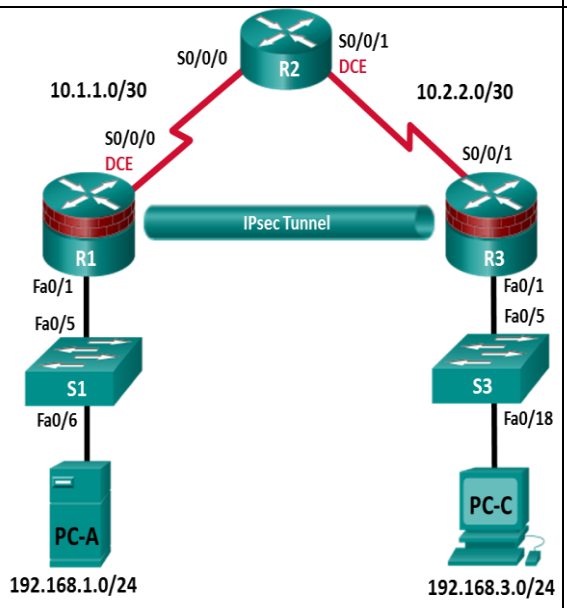
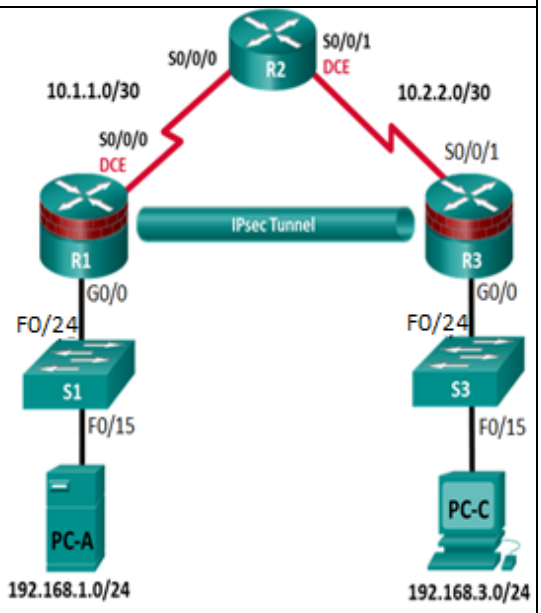
- Configuración básica como el host name, direcciones IP de interfaces y contraseñas de acceso.
- Configurar OSPF.

Parte 2: Configurar una Site-to-Site VPN usando Cisco IOS

- Configurar los parámetros de IPsec VPN en R1 y R3.
- Verificar la configuración de site-to-site IPsec VPN.
- Probar operaciones IPsec VPN.

Parte 3: Configurar una Site-to-Site VPN usando CCP

- Configurar los parámetros IPsec VPN en R1.
- Crear una configuración espejo par R3.
- Aplicar la configuración a R3.
- Verificar la configuración.
- Probar la configuración VPN usando CCP.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio es de suma importancia porque explica la forma en la que se puede crear una VPN entre diferentes equipos y redes. Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.1 Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.	

- Ejercicio 9.4.1.1 Configurar parámetros básico para un ASA y un Firewall usando CLI.

Objetivos:

Parte 1: Configuración básica de los equipos.

- Cablear la red según la topología.
- Configuración básica como el host name, direcciones IP de interfaces y contraseñas de acceso de todos los equipos.
- Configurar rutas estáticas, incluidas las por defecto entre los routers.
- Activar acceso HTTP y Telnet para R1.
- Configurar ip host para el PC.
- Verificar la conectividad entre los hosts, switches, y routers.
- Guardar la configuración básica actual de cada router y switch.

Parte 2: Acceder a la consola del ASA usando CLI para las configuraciones básicas.

- Acceder a la consola del ASA y ver el hardware, software, y las opciones de configuración.
- Determinar la versión del ASA, interfaces, y licencia.
- Determinar el sistema de archivos y los contenidos de la memoria flash.
- Usar CLI para configurar los parámetros básicos (hostname, passwords, reloj, etc.).

Parte 3: Configurar los parámetros básicos del ASA Settings y los niveles de seguridad de las interfaces usando el CLI.

- Configurar el hostname y el domain name.
- Configurar el login y activar los passwords.
- Establecer la fecha y el tiempo.
- Configurar las interfaces entrantes y salientes.
- Probar la conectividad al ASA.
- Configurar el acceso Telnet al ASA.
- Configurar el acceso HTTPS al ASA por ASDM.

Parte 4: Configurar el router traducción de direcciones y política de inspección usando el CLI.

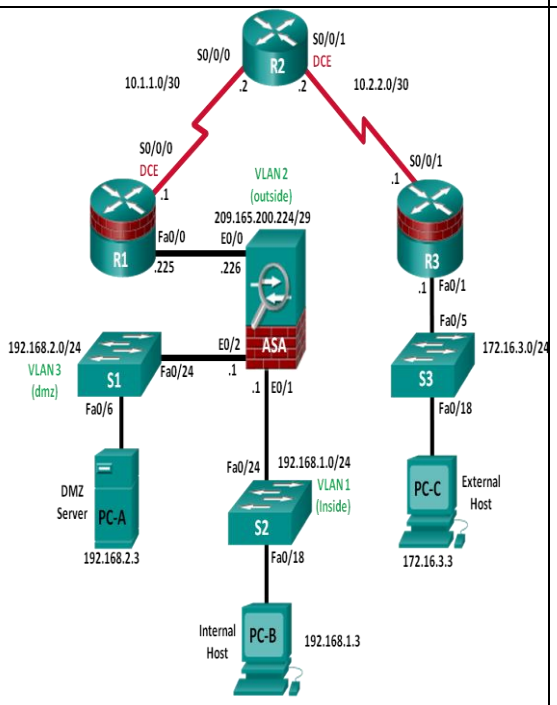
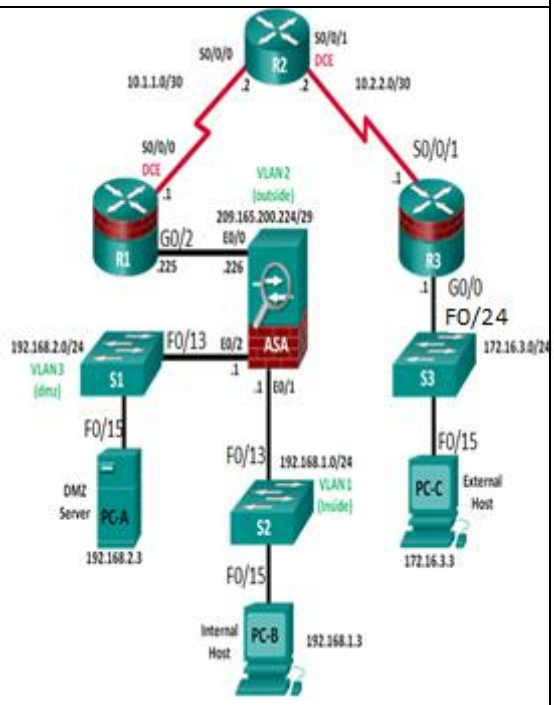
- Configurar una ruta estática por defecto para el ASA.
- Configurar (PAT) y objetos de red.
- Modificar la MPF aplicación de inspección global de política de servicio.

Parte 5: Configurar DHCP, AAA, y SSH

- Configurar el ASA como un servidor/cliente DHCP.
- Configurar autenticación local de usuarios AAA.
- Configurar acceso remoto SSH al AAA.

Parte 6: Configurar DMZ, NAT estática, y ACLs

- Configurar la interfaz DMZ VLAN3 en el ASA.
- Configurar la NAT estática para el servidor DMZ.
- Configurar una ACL para permitir el acceso al DMZ para los usuarios de Internet.
- Verificar el acceso al servidor DMA para usuarios externos e internos.

Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio engloba una gran cantidad de conceptos recogidos durante todos los anteriores por separado, por lo que resulta ser un ejercicio excelente para que los alumnos prueben cantidad de aspectos de diferentes módulos.	

- Ejercicio 10.8.1.1 CCNA Security Laboratorio

Objetivos:

Parte 1: Crear una política básica de seguridad.

Parte 2: Configuración básica de los equipos.

Parte 3: Configurar acceso administrativo al router de forma segura.

- Configurar contraseñas encriptadas y un mensaje de login.
- Configurar el timeout para el EXEC en consola y las líneas vty.
- Configurar tasa de fallos del login y mejoras del login vty.
- Configurar acceso SSH y desactivar Telnet.
- Configurar autorización de autenticación local y cuenta de usuario AAA.
- Asegurar el router contra ataques de login, además de asegurar la imagen IOS y el archivo de configuración.
- Configurar un router servidor NTP y otro cliente NTP.
- Configurar reportes syslog en el router y un servidor syslog en un host local.

Parte 4: Configurar una Site-to-Site VPN entre ISRs

- Configurar una IPsec site-to-site VPN entre R1 y R3 usando CCP.

Parte 5: Configurar un ZBF e IPS.

- Configurar ZBF en un ISR usando CCP.
- Configurar IPS en un ISR usando CCP.

Parte 6: Seguridad de red en switches

- Configurar passwords y un mensaje de login.
- Configurar la gestión del acceso de VLAN.
- Securizar los puertos de acceso.
- Protección frente a ataques STP.
- Configurar seguridad de puertos y desactivar puertos no usados.

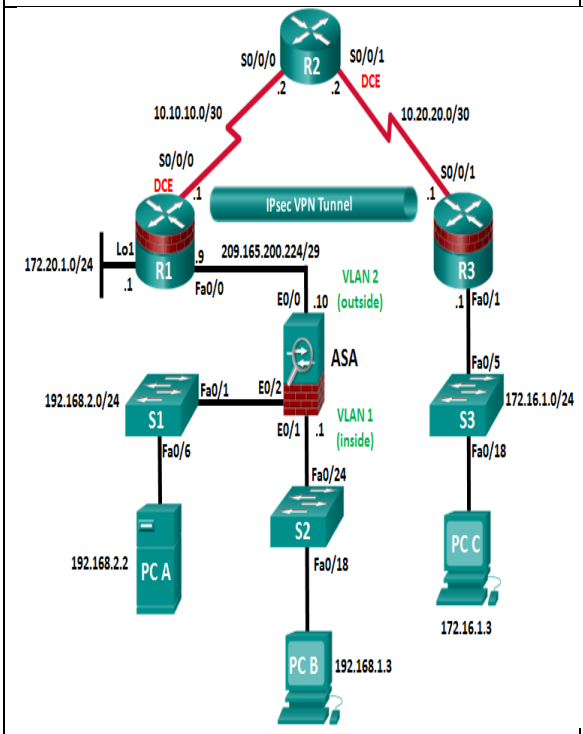
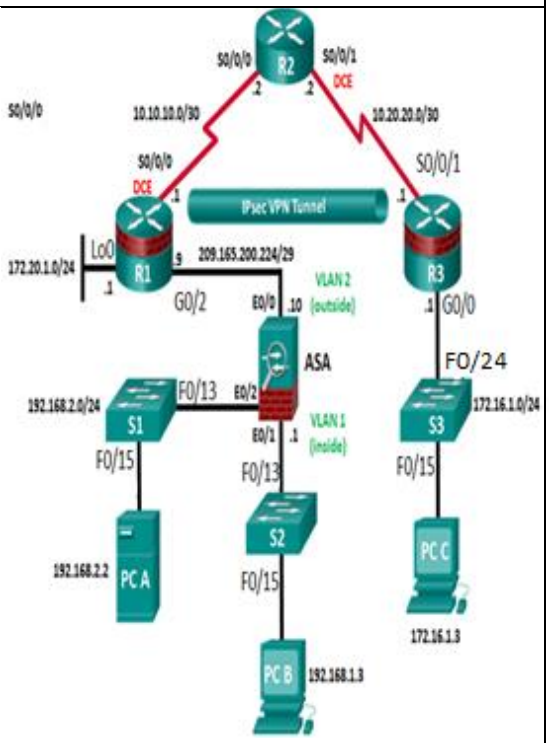
Parte 7: Configuración básica del ASA y del Firewall

- Configurar parámetros básicos, passwords, fecha, y tiempos.
- Configurar las interfaces entrantes y salientes de las VLAN.
- Configurar PAT para la red interna.
- Configurar un servidor DHCP para la red interna.
- Configurar acceso administrativo vía Telnet y SSH.
- Configurar una ruta por defecto para el ASA.
- Configurar autenticación de usuarios local mediante AAA.
- Configurar DMZ con NAT estática y ACL.
- Verificar la traducción de direcciones y la funcionalidad del firewall.

Parte 8 Configurar DMZ, NAT estática, y ACLs.

Parte 9: Configurar clientes del ASA con acceso remoto mediante SSL VPN.

- Configurar acceso remoto SSL VPN usando ASDM.
- Verificar el acceso SSL VPN al portal.

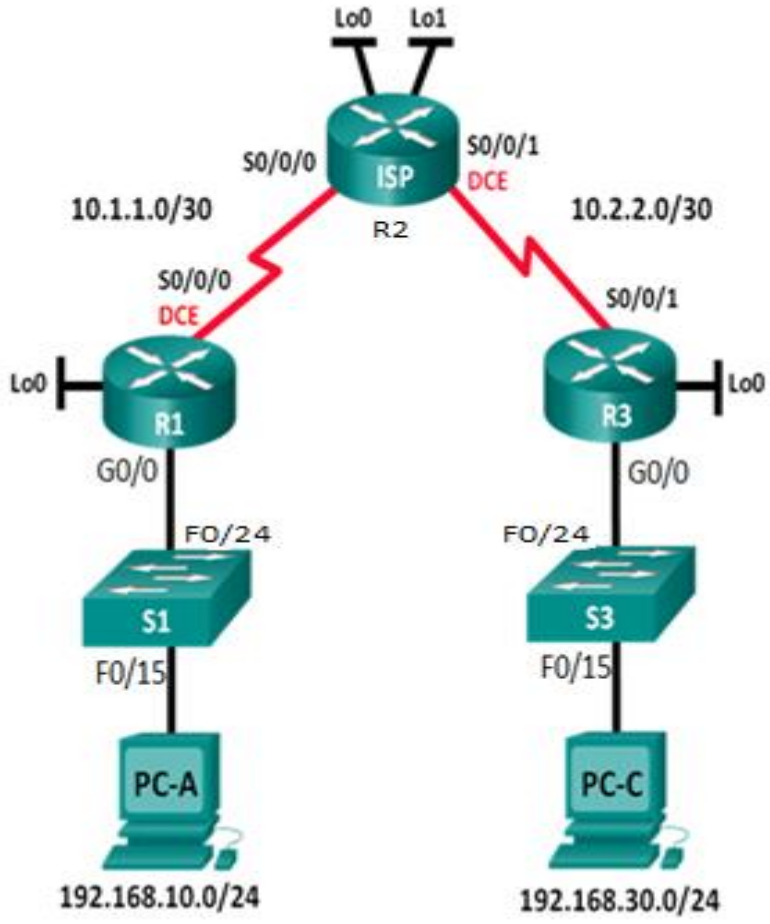
Imagen Original	Imagen Nueva
	
Se han modificado las interfaces.	
Este ejercicio supone el repaso completo a todos los conceptos vistos por los alumnos en la curricula de CCNA Security, además de muchos otros de la de Routing & Switching, por lo que es una excelente prueba para conocer las capacidades de los alumnos.	

5.3 CONFIGURACIONES BASE PARA LOS EQUIPOS

A continuación se detalla la configuración base de los equipos del laboratorio para un ejercicio en concreto, sin centrarse en aspectos más complejos de seguridad, algo que se verá en el capítulo 5.5.1 de esta memoria, sino en sus aspectos más básicos, es decir, como se encuentran los alumnos los equipos al comenzar su laboratorio.

5.3.1 CONFIGURACIONES BASE INICIALES

Por ejemplo, para el ejercicio 9.2.2.7 del módulo 2 de Routing and Switching, nos encontramos los equipos sin configuración alguna, pues los aspectos configurables de seguridad de usuarios [39] se realizan en el Access Server, que es el que les da acceso final a los equipos del laboratorio.



Ejercicio 9.2.2.7 Módulo CCNA Routing and Switching

Los router 1 y router 3 cuentan con la siguiente configuración inicial, la que se encontrarán los alumnos por defecto y que queremos mostrar en la memoria como ejemplo:

```
version 15.1
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
no service password-encryption
!!
!
ip cef
no ipv6 cef
!
!
license udi pid CISCO1941/K9 sn FTX1524YQ1J
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
```

```
!
end
```

Cada vez que un alumno termina su sesión, los routers se reinician de forma que vuelven a su configuración inicial, la mostrada anteriormente, de cara al siguiente alumno que lo vaya a utilizar. No es necesario introducir ningún comando en los mismos, pues una vez reiniciado, no guarda la configuración anterior y baja todas las interfaces.

Los switches por su parte, una vez reiniciados muestran un aspecto bastante similar a lo visto anteriormente en los routers, salvo por el hecho de que sus interfaces no se bajan automáticamente, por lo que es necesario hacerlo de forma manual o mediante un simple script:

```
S1(config)#interface range fastEthernet0/1-24
S1(config-if)#shutdown
S1(config-if)#interface ranfe gigaEthernet0/0-1
S1(config-if)#shutdown
S1(config-if)#exit
```

5.3.2 COMANDOS PARA VLANS

Si queremos establecer el direccionamiento de las VLANs (95, 96 y 97) que hemos reservado para establecer conexiones indirectas entre los routers y el ASA, se tienen que configurar primeramente los switches creando las VLANs, dejándolas reservadas.

```
S1(config)#vlan 95
S1(config)#name profesores95
S1(config)#vlan 96
S1(config)#name profesores96
S1(config)#vlan 97
S1(config)#name profesores97
```

Por ejemplo, para establecer el tráfico para R1-SW1-ASA para la VLAN 95, es necesario asociar dos puertos del switch 1 a la VLAN deseada para establecer un enlace directo entre router y ASA:

```
S1 (config)#interface range fastEthernet 0/22-23
S1 (config-if)#switchport mode access
S1 (config-if)#switchport access vlan 95
```

Se utilizan en el anterior ejemplo los puertos fastEthernet 0/22-23 del switch para establecer el enlace, aunque siguen quedando libres los puertos del 15 al 21 de cada switch. Recordamos que los 12 primeros están reservados a las conexiones entre switches, el 13 y 14 con el ASA, y el 24 con el router de igual numeración al switch.

Con el objetivo de incrementar la seguridad en una red LAN, es posible implementar seguridad de puertos en los switches de capa de acceso, de manera de permitir que a cada puerto se conecte sólo la estación autorizada. Para ello, Cisco provee port security, un mecanismo bastante potente y sencillo que resumiré a continuación.

Dirección MAC segura estática

- Se configura manualmente.
- Se agrega a la tabla de direcciones MAC.
- Se guarda en la *running-config*.
- Se puede hacer permanente guardando la configuración.

Dirección MAC segura dinámica

- Se aprende del tráfico que atraviesa la interfaz.
- Se la guarda en la tabla de direcciones MAC.
- Se pierde cuando se reinicia el equipo.

Dirección MAC segura sticky, la utilizada en la configuración de ejemplo anterior

- Se la puede configurar de forma manual o dinámica.
- Se la guarda en la tabla de direcciones MAC.
- Se almacena en la *running-config*.
- Se puede hacer permanente guardando la configuración.

La principal ventaja de las direcciones sticky en contraposición con las dinámicas es que éstas últimas se agregan al fichero running-config. Así nos evitamos escribir un montón de direcciones MAC de manera estática pero aún podemos guardarlas en el archivo de configuración de manera que se mantengan inclusive si el switch se reinicia. Dos aspectos importantes a tener en cuenta:

- Si se habilitan las direcciones MAC sticky y ya había direcciones aprendidas de forma dinámica, éstas pasan al running-config y todas las nuevas que se aprendan también se agregan allí.
- Si se deshabilitan las direcciones MAC sticky todas las que hubiera pasan a ser dinámicas y se borran del running-config. Además, todas las que se aprendan también serán dinámicas.

En el caso de que se produzca una violación, ya sea por superar el número de direcciones MAC permitidas o porque una MAC aprenda de otro puerto, se pueden tomar las siguientes acciones

- Protect: una vez que se alcanzó el máximo de direcciones MAC en un puerto, todo el tráfico de orígenes desconocidos es descartado. No obstante, se continúa enviando el tráfico legal normalmente. No se notifica al administrador de esta situación.

- Restrict: el mismo comportamiento que el caso anterior pero con la diferencia que se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.
- Shutdown: en este caso el puerto se da de baja dejándolo en estado err-disabled, deshabilitado por error. Además se envía un aviso al administrador mediante SNMP, se registra el evento en el syslog y se incrementa el contador de violaciones.
- Shutdown VLAN: la única diferencia con el caso anterior es que se deshabilita la VLAN en ese puerto en lugar de dar de baja el puerto completo. Es particularmente atractivo para los puertos de trunk.

5.4 INSTALACIÓN DEL KIT DE LABORATORIO FÍSICO

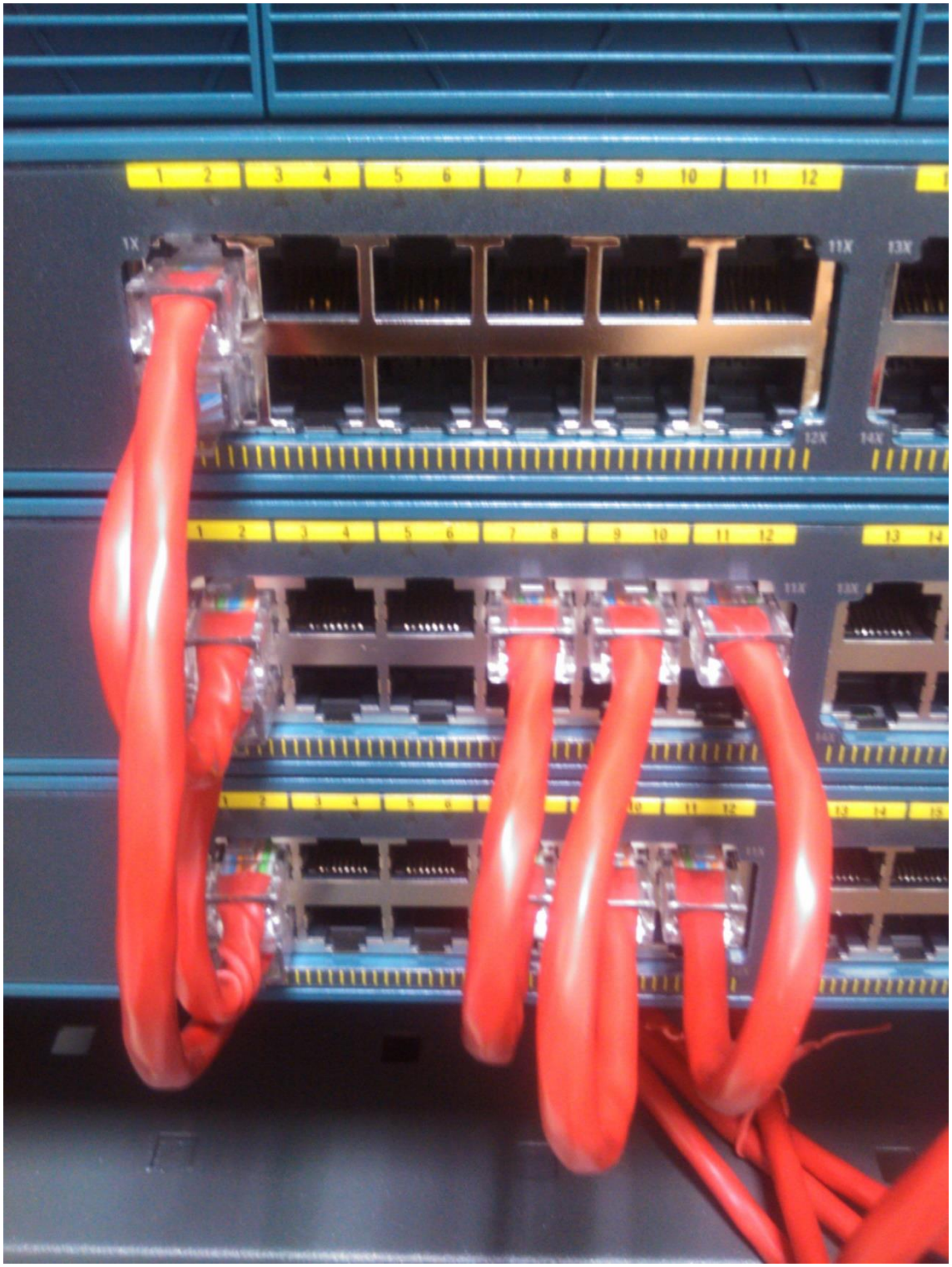
El laboratorio físico cuenta con dos escenarios o dos kits, cada uno de ellos formado por tres routers 2911 CISCO2911/K9, uno de los cuales, el de arriba, tiene características de seguridad CISCO2911-SEC/K9, tres switches 2960 de 24 puertos WS-C2960-24TT-L y un firewall ASA 5505 ASA5505-BUN-K9.

Tanto los switches como los routers incorporan un par de sujeciones que son necesarias atornillar a ambos lados de los mismos para posteriormente servir de anclaje en el armario y dejarlo fijado, mediante otro proceso de atornillado.

Los routers nombrados como R1 y R3 son los elegidos para tener características de seguridad, tanto en el laboratorio físico como en las topologías virtuales. Tomando desde abajo hacia arriba su nomenclatura, es decir R1 estará debajo de R2 y éste de R3, y de igual forma los switches.

Las tarjetas en los switches se han colocado de forma que cuadren las interfaces con la nomenclatura de las topologías, pues cuenta con diferentes posiciones para introducir las tarjetas de conexiones que hubieran denotado otra nomenclatura final.

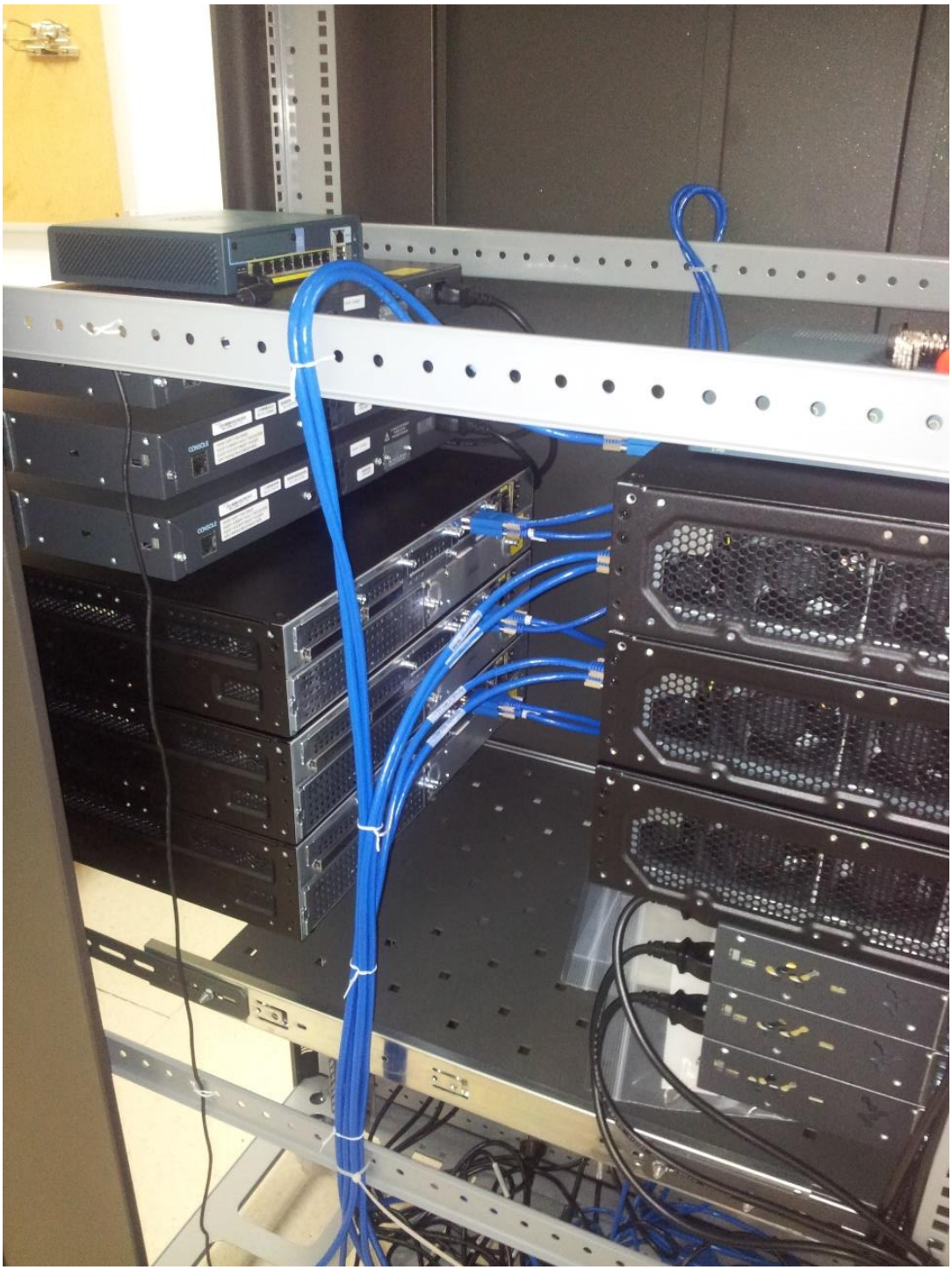
Se estableció para el kit 1 que las conexiones entre los switches se realicen por delante, entre los switches y el ASA por el lateral derecho del armario, y entre switches y routers por debajo de los equipos hasta las conexiones traseras de los propios routers. Las conexiones serie entre los diferentes routers se encuentran sujetas en la parte posterior a la izquierda aprovechando los andamios del armario.



Kit 1 - Switches

Kit 1 – Vista General frontal de ASA, Routers y Switches.

Kit 1 – Vista frontal



Conexiones serie del kit 1 y el Kit 2

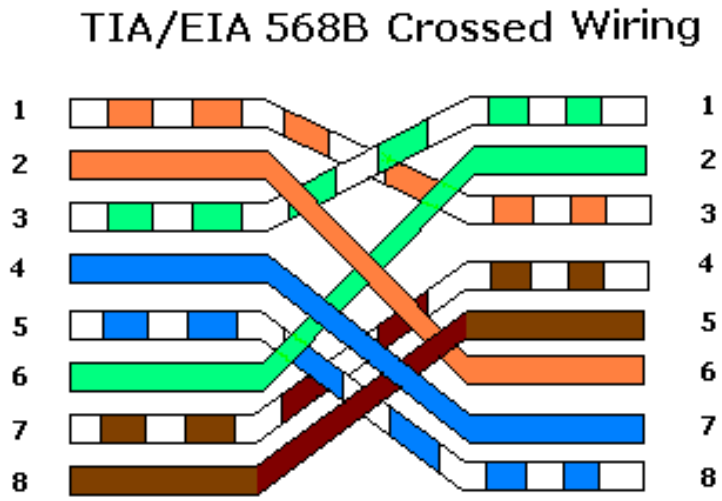
En el Kit 2 por problemas a la hora del montaje de los equipos, tenemos una separación de una unidad del rack entre los diferentes swtiches, por lo que para aprovechar este hecho inesperado, las conexiones entre los puertos giga Ethernet del switch con los giga Ethernet de los routers pasarán por ese espacio libre. El resto de conexiones se encuentran colocadas de igual forma que las del kit 1.

Kit 2 – ASA, Swtiches y Routers aún sin las conexiones

Kit 2 – Vista Frontal con las conexiones

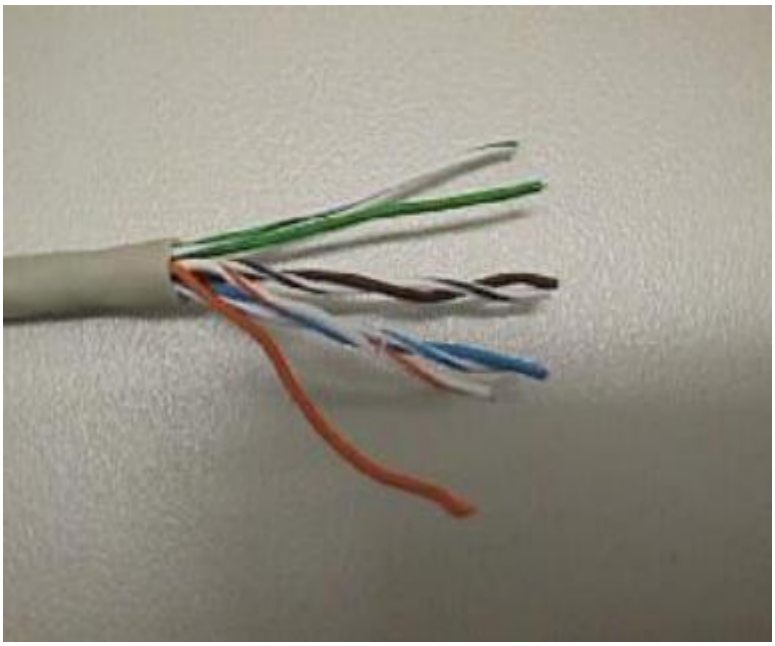
En las conexiones cruzadas se cruzan los 4 pares para tener mayor velocidad de conexión, usando cables de categoría 6 (cables rojos) para las conexiones entre los mismos switches y de categoría 5 (cables negros) para el resto de conexiones entre switches y routers, y

switches y el asa. De esta forma es más sencillo distinguir visualmente las conexiones cruzadas, de color rojo, de los directos, de color negro.



Disposición interna de los cables para realizar las conexiones cruzadas

Ha sido necesaria la elaboración de los cables de red RJ-45, tanto cruzados como directos, para realizar el conexionado de los dos escenarios físicos. Para la realización de latiguillos con conectores modulares RJ-45 se utiliza cable flexible UTP (Unshielded Twister Pair) de categoría 5 y categoría 6 que se compone de 8 conductores trenzados par a par y todos ellos recubiertos por una funda externa de protección.. De esta forma, en el interior del cable nos encontramos con la siguiente disposición de los conductores.

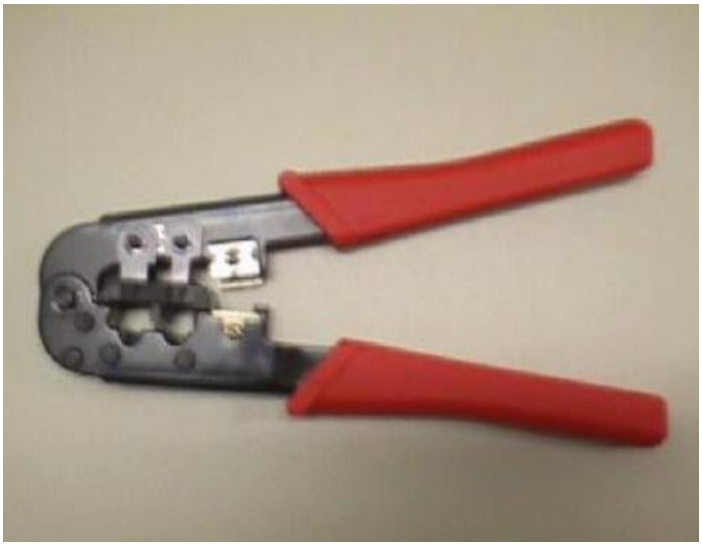


Interior de un cable de red RJ-45

Sus colores son:

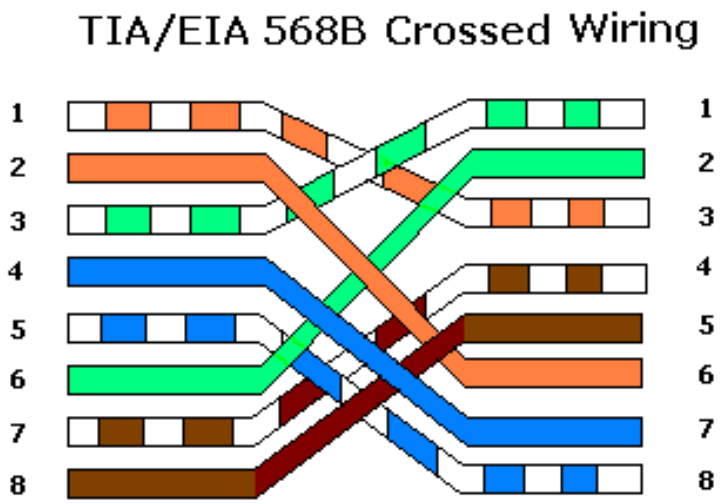
- Naranja.
- Blanco / Naranja.
- Verde.
- Blanco / Verde.
- Azul.
- Blanco / Azul.
- Marrón.
- Blanco / Marrón.

Para la elaboración del cable se corta un trozo según la longitud que deseemos o hayamos estipulado para la conexión en concreto. Se pela el recubrimiento externo del cable en una longitud aproximada de 1,5 cm en el extremo donde vayamos a colocar el conector modular RJ-45. Al realizar este proceso hay que tener mucho cuidado para no dañar, o cortar ligeramente los conductores internos. En este proceso utilizaremos la siguiente herramienta, unas tenazas de crimpar:



Crimpadora

Tras esto, se colocan los conductores interiores, con su cubierta individual, uno al lado del otro en el mismo plano para poder introducirlos en el conector modular según el orden es que muestra la figura, de forma que sin cruzados, un extremo del cable deberá tener el orden de sus conductores de la parte izquierda de la imagen, y el otro extremo el orden de los colores de la parte derecha de la imagen. En el caso de ser directos se seguirá el mismo patrón, por ejemplo el de la izquierda en ambos extremos.



Disposición interna de los cables para realizar las conexiones cruzadas

Una vez que tenemos el orden claro de los conductores se estiran de forma que se puedan cortar con la crimpadora para quedar todos de la misma longitud y así, poder introducirlos en el orden deseado en el conector RJ-45.

Conector RJ-45

Coger el conductor modular RJ-45 y con los contactos hacia la parte superior la pestaña hacia la parte inferior) introducir en él los conductores internos del cable hasta llegar al fondo. Quedando los conductores alineados en el extremo superior del conector modular y directamente debajo de los contactos dorados. Observar que todos los conductores quedan perfectamente introducidos hasta el fondo y que el orden de los cables es el correcto. De igual forma es recomendable introducir parte de la carcasa externa del cable para que la crimpadora pueda ajustar de mejor forma la conexión y evitar que quede, literalmente, colgando en el futuro.

Introducir el conector modular RJ-45 en la boquilla de las tenazas de crimpar y presionar con fuerza hasta que los contactos dorados, conocidos como pines, ocho en total, uno por cada conductor, queden perfectamente introducidos, asegurando la perfecta unión con los conductores en el interior del conector.

Acción de crimpar con mayor detalle

De esta forma se realiza un extremo del cable, siendo necesario hacer el otro extremo para finalizar el cable.

En cuanto a los problemas encontrados en el montaje del laboratorio físico, hay que destacar que el armario en el que se encuentran los dos kits tiene puertas que dificultan en ocasiones el manejo de los equipos, y aunque se quiten, es difícil hacerlas encajar. También las medidas de los anclajes del armario para los switches y routers son diferentes, por lo que un kit no tiene huecos entre sus equipos mientras que el otro kit cuenta con un hueco vacío entre switches. Los cables serie DTE y DCE no tienen un indicador claro de cual es cual, es necesario abrirlos para ver cuál es hembra o macho, conectores Winchester que no indican el tipo de conexión (las hembras se utilizan para simular DCE y los machos DTE), por lo que hay que llevar un riguroso trabajo de conexionado.

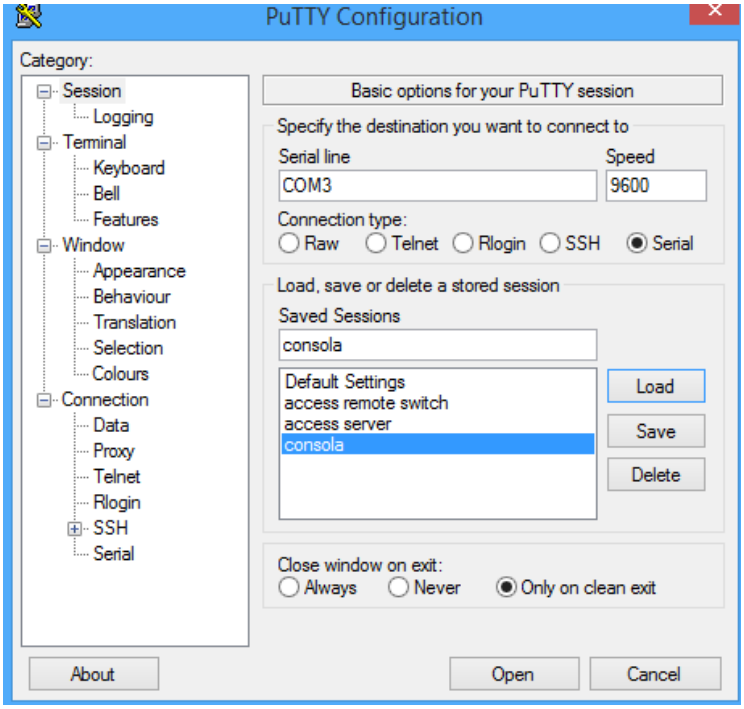
El conector de la izquierda representa DCE y es hembra, el de la derecha DTE y es macho.

A la hora de crimpar los cables, el cable rojo de categoría 6 utilizado para conexiones cruzadas entre los switches, tenían un separador central que dificultó su labor.

5.5 CONFIGURACIÓN DEL ACCESS SERVER

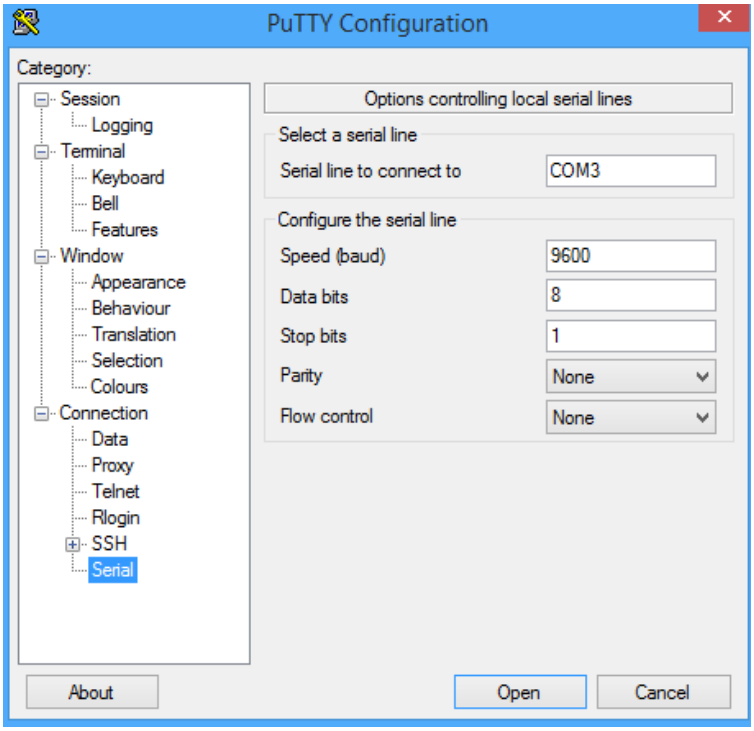
La configuración del Access Server es el punto más importante de este trabajo, pues mediante el mismo es posible conectarse a los equipos del laboratorio de forma remota y establecer los principios de seguridad adecuados al tipo de usuario que decida acceder. Por eso, primeramente se crearon usuarios (en mi caso y en el de los profesores) con permisos de administración para la gestión del Access Server y su futura configuración, tanto del propio equipo como los del kit del laboratorio. Más tarde, se crearon usuarios sin permisos de administración para los futuros alumnos, quienes se conectarían en un futuro a los puertos asíncronos del Access Server en los que se encuentran los equipos del kit.

Para empezar, fue necesario conectar un PC portátil al Access Server mediante puerto de consola, para comenzar a realizar su configuración básica. Esta conexión requirió buscar los drivers adecuados para que el ordenador reconociera el puerto de consola, en este caso COM3. Para acceder por consola, y más tarde por SSH [38], fue necesario utilizar la herramienta Putty, un cliente de red que soporta los protocolos SSH, Telnet y Rlogin, y sirve principalmente para iniciar una sesión remota con otra máquina o servidor. Es de licencia libre y está diseñado y mantenido principalmente por Simon Tatham desde Gran Bretaña. A pesar de su sencillez, es muy funcional y configurable, para este caso en concreto se configuró de la siguiente forma:



Putty – Acceso por consola al Access Server

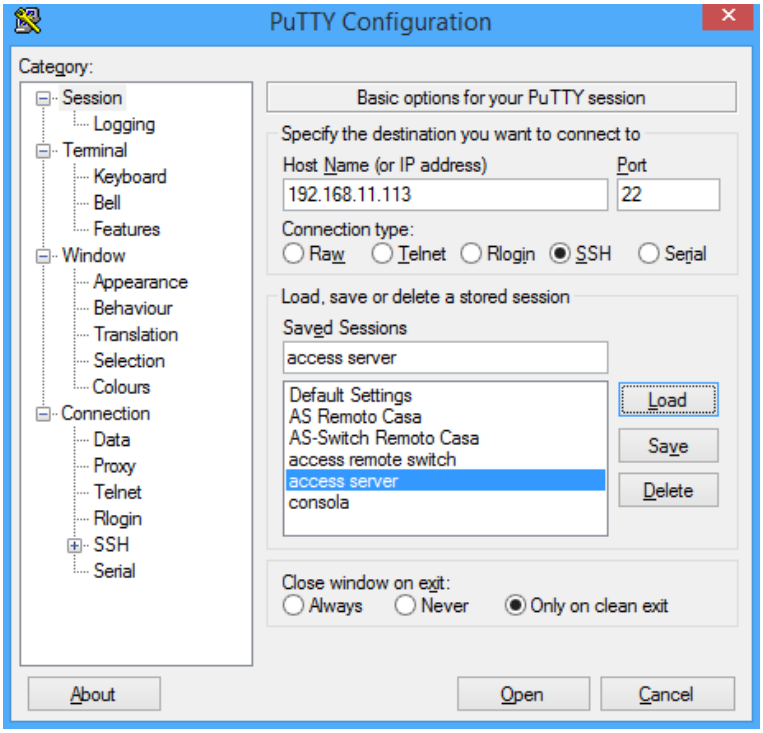
Conexión serie, velocidad 9600, a través del puerto COM3. Las opciones de la conexión serie se establecieron de la siguiente forma:



Putty – Acceso por consola al Access Server

Una vez conectados sin mayores problemas, se configuraron los parámetros básicos del Acces Server, tales como el nombre de host, el dominio, nombre de usuario y contraseña encriptada. Además, se tuvieron que configurar las líneas telnet, vty, ssh y los privilegios de usuario para poder acceder al Access Server de forma remota, desde la red del departamento, mediante la herramienta Putty por protocolo SSH, sin necesidad de tener que estar conectado mediante consola. Con la siguiente configuración básica, cambiamos el hostname, establecemos un usuario local con privilegios de nivel 15 y establecemos la dirección ip a la que nos conectaremos mediante SSH, configurado en las líneas vty 0 4 con login de la base local:

```
hostname AS
no ip domain lookup
ip domain name fi.upm.es
username tfg privilege 15 secret 5 XXX
service password-encryption
crypto key generate rsa 1024
ip ssh version 2

interface GigabitEthernet0/1
ip address 192.168.11.113 255.255.255.0
no shutdown

banner motd ^CBIENVENIDOS^C

line vty 0 4
login local
transport input ssh
```



Putty – Acceso remoto al Access Server desde la Facultad

Para seguir avanzando, este Access Server se conectó mediante OCTAL-ASYNC-CABLE a un switch similar a los que se encuentran en el laboratorio con el fin de configurar el Access Server de forma que nos diera acceso remoto a dicho Switch mediante la configuración de sus líneas y puertos, en este caso se utilizó la interfaz Gigabit Ethernet 0/1 del Access Server, la cual estaba conectada al switch. Pudiendo acceder a este switch a través del propio Access Server mediante el comando SSH ssh -l tfg:66 192.168.11.113, donde se indica la dirección ip de salida del Access Server hacia el Switch, la línea 66 en la que se encuentra conectado y el usuario "tfg" para su autenticación.

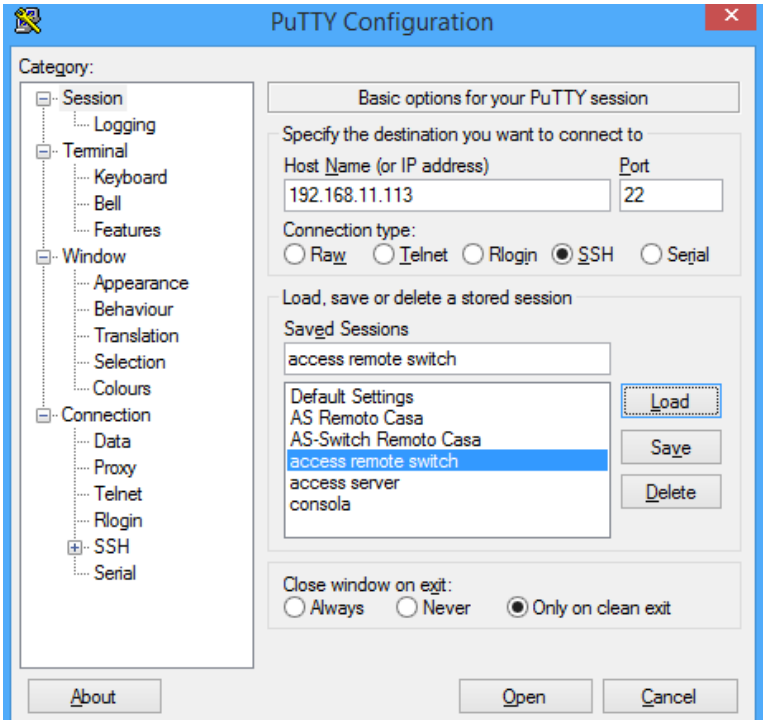
Lo vemos mejor en los comandos respectivos de configuración del Access Server, estableciendo para el puerto 2066 las 16 líneas asíncronas, siendo la primera de ellas la 66 la que requiere darle acceso mediante SSH con autenticación de usuario de la base local[34][35]. El primer comando permite conectar el puerto 2066 a un grupo de líneas, en este caso las 16 proporcionadas por los cables asíncronos. El resto de comandos permiten el acceso a la línea 66, por la primera línea asíncrona física, mediante vía SSH con autenticación local:

```
ip ssh port 2066 rotary 66 81

line 1/0
login local
```

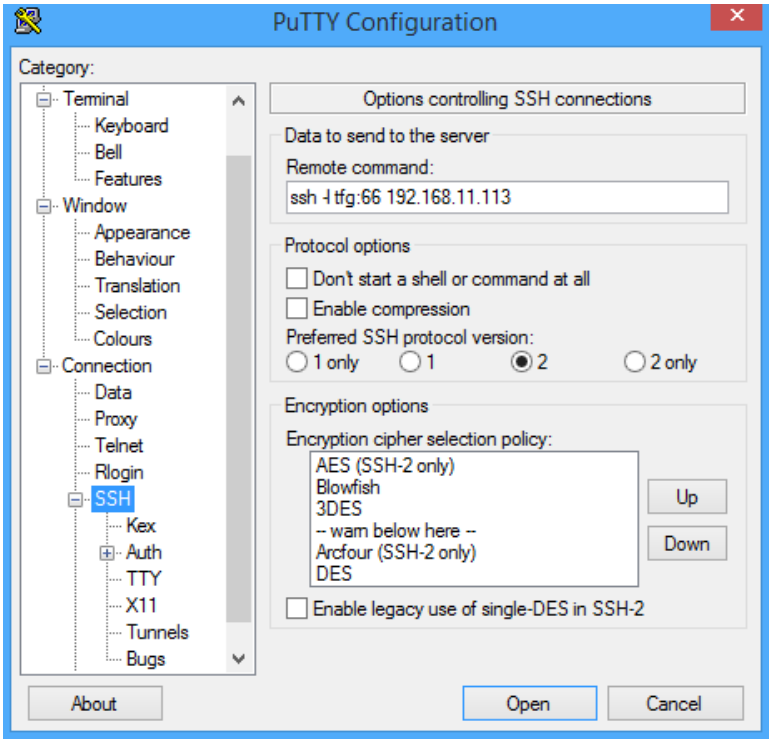
```
rotary 66
transport input ssh

line 1/1
login local
rotary 67
transport input ssh

line 1/2
login local
rotary 68
transport input ssh

line 1/3
login local
rotary 69
transport input ssh

line 1/4
login local
rotary 70
transport input ssh

line 1/5
login local
rotary 71
transport input ssh

line 1/6
login local
rotary 72
transport input ssh

line 1/7
login local
rotary 73
transport input ssh

line 1/8
login local
rotary 74
transport input ssh

line 1/9
login local
```

```
rotary 75
transport input ssh

line 1/10
login local
rotary 76
transport input ssh

line 1/11
login local
rotary 77
transport input ssh

line 1/12
login local
rotary 78
transport input ssh

line 1/13
login local
rotary 79
transport input ssh

line 1/14
login local
rotary 80
transport input ssh

line 1/15
login local
rotary 81
transport input ssh
```

En Putty será necesario incluir los siguientes comandos para evitar pasar por el Access Server y acceder directamente al switch:



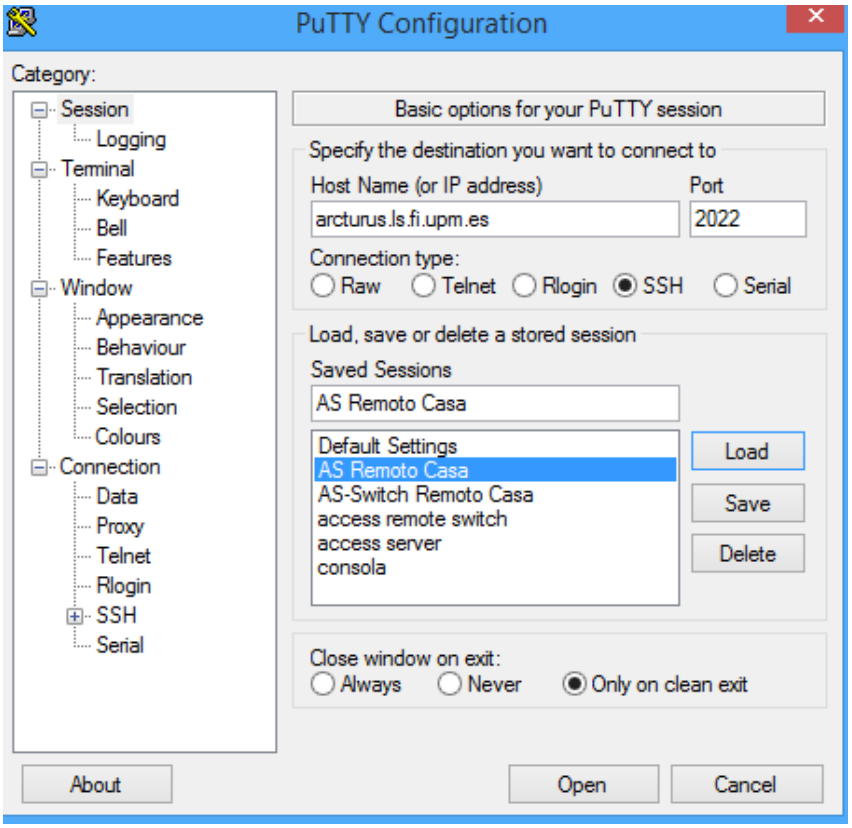
Putty – Acceso remoto a Switch desde la Facultad



Putty – Acceso remoto a Switch desde la Facultad

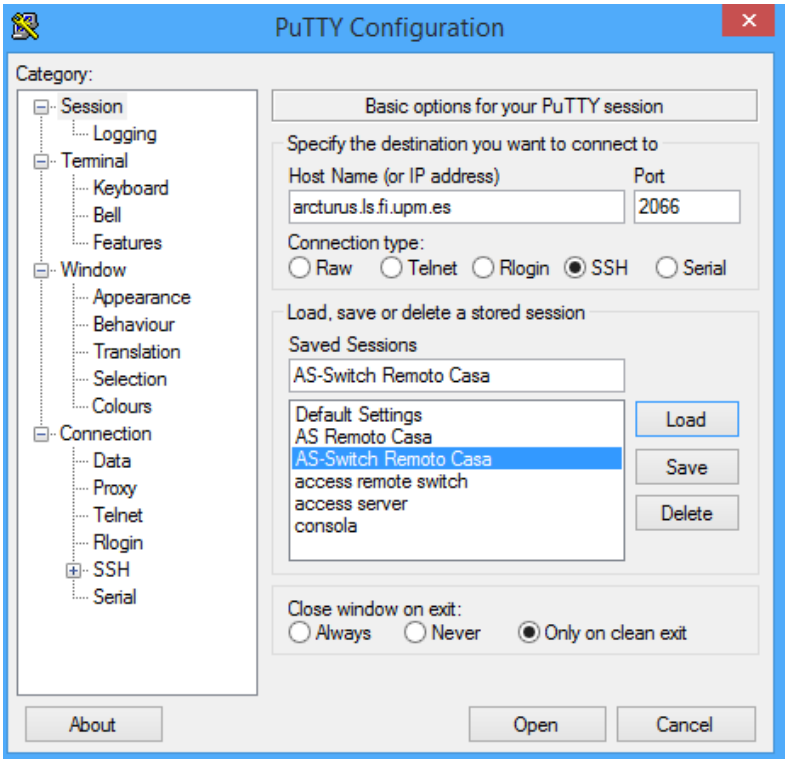
El siguiente paso consistió en acceder al propio Access Server de forma remota desde una red externa a la facultad, sin requerir tampoco el estar conectado a la VPN de la universidad, su red privada virtual. Para ello, fue necesario configurar un usuario, tfg, su

respectiva contraseña, nombre de dominio, protocolo SSH en su versión número 2 y aplicar la seguridad de autenticación a las líneas vty, algo que ya hemos visto en los comandos de los apartados anteriores. Además de una ruta que de salida (ip route 0.0.0.0 0.0.0.0 192.168.11.254) a todo el tráfico externo a la facultad. Pudiendo acceder mediante la herramienta Putty de la siguiente forma:



Putty – Acceso remoto al Access Server desde red externa a la Facultad

Mientras que para conectarnos desde una red externa a la de la facultad al switch conectado al Access Server, solamente es necesario indicar el puerto, 2066, en el que se encuentra conectado el switch:



Putty – Acceso remoto al Switch desde red externa a la Facultad

El Access Server sirve de puente al resto de equipos del laboratorio, es decir, los de los dos kits físicos, mediante el cable OCTAL-ASYNC-CABLE. Los alumnos que deseen acceder a estos equipos para realizar sus respectivos ejercicios necesitarán un usuario, contraseña y su dirección IP, previamente proporcionada mediante la aplicación que realizará otro alumno del departamento. De forma que el Access Server compruebe la validez de ese par usuario/contraseña y permita el tráfico mediante una ACL, lista de acceso, a su conexión. Así se ve que la autenticación y autorización de los alumnos se realiza en el Access Server, pese a que ellos no van a acceder a él, sino a los equipos del kit 1 o del kit 2.

El mayor problema que apareció en esta etapa de configuración del Access Server, y en el cual perdimos algo de tiempo, fue el darle salida al Access Server para el tráfico externo y así poder acceder a los equipos desde una red externa a la de la Facultad, labor que quedo a cargo de mi tutor al requerir contraseñas y configuraciones de la propia red de la facultad.

5.5.1 OPCIONES DE SEGURIDAD

A la hora de establecer la seguridad en el Access Server y en el resto de equipos, se barajaron 3 opciones:

- Usuarios con privilegios [41][42][43][44][44][45][46][47][50]
- Event Manager (EEM)[48][49][51][54]
- AAA[40][52]

Finalmente se optó por una combinación de usuarios/contraseña con privilegios y Event Manager, descartando utilizar la autenticación y autorización AAA de los usuarios mediante servidores TACACS+ [33] y RADIUS por que hacían imposible la conexión mediante SSH de forma correcta, además de que no funcionaba correctamente en los switches[53] y requería de un total de 14 servidores que se encargarán de sus funciones. A continuación se explican las 3 opciones de seguridad principales:

La posibilidad de crear diferentes niveles de privilegio nos permite delimitar el acceso que tienen los usuarios sobre la administración del equipo. Existen 16 niveles de privilegio, los niveles 0,1 y 15 tienen configuraciones y comandos predefinidos, mientras que los niveles entre el 2 y el 14 son completamente personalizables.

Es importante apuntar que si tenemos un usuario asociado a un nivel de privilegio, por ejemplo el nivel 14, este usuario va a tener acceso a los comandos definidos dentro de ese nivel 14, así como también a los comandos definidos en los niveles inferiores desde el 0 hasta el 13.

De forma que, como administradores, se pueden configurar todos los comandos que tendrán disponibles los usuarios de nivel 14, diferenciando entre los 4 modos disponibles: enable, configuración de router, líneas e interfaces. Ejemplo de la creación de un usuario con privilegio de nivel 14 y con contraseña para acceder al modo enable, además de permitirle los comandos para acceder al modo de configuración, y de interfaz:

```
username admin privilege 15
username alumno privilege 14
enable secret level 14 pass
privilege interface level 14 ip address
privilege configure level 14 interface
privilege exec level 14 configure terminal
```

El borrado de un usuario se realiza de forma sencilla con el prefijo “no”:

```
no username alumno
```

En nuestro laboratorio utilizamos dos usuarios, el de administración con privilegios 15 para mi propio uso y el de los profesores, y luego, el usuario de alumnos, obviamente el que usarán los propios alumnos para acceder al laboratorio, sin permisos de administración.

EEM (Event Manager) es un componente de software de Cisco IOS, XR y NX-OS que da altas capacidades de administrador siguiendo y monitorizando el dispositivo Cisco en cuestión. EEM permite automatizar muchas tareas comunes de la configuración de un dispositivo, además de monitorizar y prevenir ciertas acciones. En nuestro laboratorio, resulta posible su utilización en routers, lo cual disminuye la tarea frente al uso de privilegios, los cuales son necesarios en los switches al no aceptar Event Manager.

Hay dos tipos de EEM, los applets, que son un conjunto de comandos de la CLI, y scripts, acciones codificadas en TCL.

Aquí encontraremos algunos ejemplos de applets y vamos a poner en nuestras mentes que sólo puede tener un evento por subprograma con acciones simples o múltiples se ejecutan en secuencia.

EEM permite detectar ciertos eventos que surgen en la actividad de los dispositivos:

- SNMP: Seguimiento objetos de tipo SNMP.
- Syslog: -Responde a varios mensajes de registro del sistema, lo que permite hacer expresiones regulares.
- Contador: Monitoriza y responde a la interfaz del usuario cuando la configuración supera cierto umbral establecido.
- Eventos del CLI: Detección de entrada CLI para una expresión regular.
- Ninguno: Este detector evento es para probar EEM usando "event manager run".
- Timers: Eventos de tiempo.
- IP SLA y los flujos netos de eventos.

Las acciones que puede tomar EEM son:

- Enviar un mensaje de correo electrónico al administrador o al propio usuario.
- Permitir o inhabilitar un comando de Cisco.
- Generar Trampas SNMP.
- Reiniciar el router.
- Generación de mensajes syslog priorizados.
- El cambio a un procesador secundario en una plataforma redundante.
- Solicitud de información de sistema cuando se produce un evento (como muestra para el soporte técnico o uso histórico de la CPU, entre otros).

A continuación se mostrarán varios ejemplos del funcionamiento de EEM. El primer ejemplo impide a los usuarios realizar, por ejemplo, un ping a la dirección 1.1.1.1, mostrándoles un mensaje informativo:

```
event manager applet noping
event cli pattern "ping 1.1.1.1" sync no skip yes
action 1.0 syslog msg "commnad is bypassed try again later"
```

Ya empezamos a ver la utilidad de EEM de mejor forma, por ejemplo impidiendo el comando "configure terminal" para acceder al modo de configuración:

```
event manager applet noconfig
event cli pattern "configure terminal" sync no skip yes
action 2.0 cli command "enable"
```

Sucede lo mismo, por ejemplo, si queremos evitar que un alumno reinicie un equipo:

```
event manager applet DisableReload
event cli pattern "reload" sync no skip yes occurs 1
action 1.0 syslog msg "$_cli_msg has been disabled."
```

Por último, también se pueden crear scripts que levanten automáticamente las interfaces:

```
event manager applet f00-up
event track 1 state up
action 6.0 cli command "enable"
action 6.1 cli command "config t"
action 6.2 cli command "int fas 0/1"
action 6.3 cli command "no sh"
action 6.4 cli command "end"
end
```

Por otra parte, la autenticación AAA mediante RADIUS y TACACS+ quedó descartada por surgir problemas a la hora de establecer las conexiones SSH, sobre todo en los switches, por lo que se prefirió utilizar autenticación en local. No obstante, esta seguridad permite:

- Autenticación: comprueba que los usuarios y administradores sean quienes dicen ser.
- Autorización: después de la autenticar al usuario o al administrador, decide a qué recursos puede acceder o qué operaciones puede realizar.
- Registro (Accounting and Auditing): guarda el instante temporal en el que se efectúan las operaciones y acceden a los recursos.

Por su parte, TACACS es un protocolo de autenticación remota, propietario de cisco, que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes

Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red. TACACS+ es más seguro pero RADIUS tiene mejor Accounting y una mejor interfaz de programación.

Como se ha visto en las tres opciones explicadas, Event Manager es la que mejor cuadra con nuestros objetivos de impedir a los alumnos utilizar permisos administrativos y salvaguardar así el laboratorio. Resulta más rápida, cómoda y con un mayor abanico de opciones que utilizar privilegios, no obstante estos son compatibles y sumamente necesarios en los switches, donde Event Manager no funciona. La pega de los privilegios, es la necesidad de escribir la totalidad de los comandos que los alumnos han de poder utilizar, lo cual es una tarea muy larga, siendo más útil el impedir los comandos no deseados desde Event Manager.

Además de estas opciones globales de seguridad [36], también es necesario añadir listas de acceso, ACLs, para verificar la dirección IP de los alumnos. Esto es así, porque a través de la aplicación web diseñada por otro alumno del departamento, se les solicita a los alumnos la dirección IP desde la que accederán al laboratorio, para tener una mayor seguridad y saber realmente que se trata de ellos.

Se utiliza la sintaxis básica de filtrado de acceso por IP de Cisco para listas extendidas:

```
access-list access-list-number [dynamic dynamic-name [timeout
minutes]]
  {deny | permit} protocol source source-wildcard destination
    destination-wildcard
  [precedence precedence] [tos tos] [log | log-input]
    [time-range time-range-name]
[fragments]
```

La creación de estas listas de acceso da mucho juego, permitiendo solamente al usuario que ha reservado la sesión acceder al laboratorio, por ejemplo permitiendo a un equipo acceder a un rango de direcciones en las que están nuestros equipos:

```
access-list 101 permit ip 192.168.10.9 0.0.0.0 192.168.100.0
0.0.0.255
access-list 101 deny ip any any
```

El primer comando se puede acortar de la siguiente forma, pues siempre se referirá a una dirección en concreto de un equipo:

```
access-list 101 permit ip host 192.168.10.9 192.168.100.0
0.0.0.255
```

Y de igual forma si solo queremos que acceda a los equipos en concreto en vez de tener un rango disponible:

```
access-list 101 permit ip host 192.168.10.9 host 192.168.100.1
```

Para que las listas de acceso se activen, es necesario configurarlas a la entrada o a la salida de las interfaces, en este caso del Access Server para dar acceso al resto de equipos del laboratorio. Preferiblemente en la interfaz entrante es necesario configurar el comando "ip access-group 101 in", permitiendo el acceso solamente al usuario que haya reservado previamente el laboratorio.

No hay una manera de editar de forma sencilla la ACL [55] [56] [57] [58] desde la consola, lo único es intercalar sentencias y eliminar otras, ya que no se pueden sobreescribir, siendo tedioso y peligroso. Lo mejor es copiar la ACL del running-config y llevársela a otro fichero para editarla allí. Lo siguiente será quitar la ACL actual de la interfaz y después eliminarla del router y de la interfaz asociada. A continuación, copiamos las sentencias del bloc de notas para crear de nuevo la ACL y, por último, la aplicamos de nuevo a la interfaz correspondiente. El construir la ACL de nuevo sería igual que lo mostrado anteriormente, mientras que su borrado se haría:

```
no access-list 101
```

No obstante, aunque es laborioso si se puede editar una ACL. Cuando mostramos el contenido de una lista de acceso obtenemos lo siguiente:

```
10 permit ip 192.168.10.9 0.0.0.0 192.168.100.0 0.0.0.255
20 deny ip any any
```

Al leerse de esta forma, se podría intercalar alguna sentencia, por ejemplo:

```
ip access-list 101
15 permit ip 192.180.13.4 0.0.0.0 192.168.100.0 0.0.0.255
```

Quedando de la siguiente forma la ACL:

```
10 permit ip 192.168.10.9 0.0.0.0 192.168.100.0 0.0.0.255
15 permit ip 192.180.13.4 0.0.0.0 192.168.100.0 0.0.0.255
20 deny ip any any
```

De igual forma, podemos eliminar entradas de la ACL de la siguiente forma:

```
ip access-list 101
no 20
```

Quedando de la siguiente forma la ACL:

```
10 permit ip 192.168.10.9 0.0.0.0 192.168.100.0 0.0.0.255
20 deny ip any any
```

Para el caso de nuestro laboratorio, vamos a mostrar, a modo de ejemplo, como permitir una IP de un usuario, para una vez terminada su sesión, borrar su dirección y así permitir a otro usuario la entrada al laboratorio:

```
access-list 101 permit ip host 192.168.0.10 172.130.0.0
0.0.255.255
access-list 101 deny ip any any
interface fa0/0
 ip access-group 101 in
```

Mientras que este usuario se encuentre en su sesión, la ACL se verá como:

```
Extended IP Access list 101
 10 permit ip host 192.168.0.10 172.130.0.0 0.0.255.255
 20 deny ip any any
```

Una vez finalizada su sesión, se procede al borrado de su IP en la entrada de la ACL y la posterior sobreescritura de la siguiente IP del próximo alumno que vaya a acceder al laboratorio:

```
ip access-list extended 101
 no 10
 10 permit ip host 192.185.0.10 172.130.0.0 0.0.255.255
```

Así, la ACL queda de la siguiente forma durante la siguiente sesión:

```
Extended IP Access list 101
 10 permit ip host 192.185.0.10 172.130.0.0 0.0.255.255
 20 deny ip any any
```

Como se ve, se pueden editar ACLs de diferentes formas, aunque la secuencia de lectura de las mismas supone un punto importante de dificultad a la hora de su modificación, pero con un simple script en el que se borre la entrada actual de un usuario y se edite esa misma entrada con la nueva IP del nuevo usuario, sirve para controlar el acceso al laboratorio.

5.6 CONFIGURACIÓN DE LOS EQUIPOS

Los equipos, para ser fieles a los ejercicios que los alumnos han de hacer, se encuentran sin configurar, aunque naturalmente, se encuentran conectados al resto de equipos pero no hay ninguna configuración en ellos, tal y como indican sus respectivos enunciados. No obstante, es necesario establecer ciertos parámetros de seguridad para que los alumnos no puedan alterar el funcionamiento de los equipos, para ello y gracias a los privilegios se les puede denegar el acceso a ciertos comandos como el cambio de los propios

permisos, del borrado total de la configuración o cambios en las contraseñas globales que puedan afectar al departamento como administradores.

Como se ha explicado anteriormente, tenemos diferentes usuarios creados, para los profesores y para mí un usuario que permita administrar y gestionar todos los equipos del laboratorio, mientras que por otro lado está el usuario de los alumnos, sin permisos de administración y con restricciones a la hora de utilizar ciertos comandos que podrían causar problemas en todo el laboratorio. Naturalmente, cada usuario cuenta con su respectiva contraseña. En el caso de los alumnos, se realiza un filtrado de su ip mediante listas de acceso (ACLs) para asegurar que realmente es un alumno dado de alta en el laboratorio.

Resumiendo, los equipos del laboratorio se encuentran conectados entre sí según la topología establecida, aunque sin rutas establecidas. Solamente algunos comandos de seguridad que impidan a los alumnos machacar la propia configuración establecida en los mismos, sobre todo en el aspecto de seguridad. Me refiero al establecimiento de usuarios, contraseñas, eventos de EEM y las VLANs establecidas por el departamento.

5.7 AUTOMATIZACIÓN DE LOS EQUIPOS

Los alumnos han de encontrarse cada vez que acceden al laboratorio remoto, los equipos sin nada configurado, salvo algunas contraseñas y parámetros explicados en el apartado anterior, que impidan a los propios alumnos sustituir o modificar contraseñas globales o parámetros de seguridad. De forma que cada vez que la sesión de un alumno expire, se borrará todo lo realizado por el alumno en su respectivo kit y se volverá a la configuración inicial donde se añadirán usuarios y contraseñas, parámetros de seguridad del Event Manager y las VLANs, para que el próximo alumno pueda acceder sin problemas.

Se guardará el fichero de configuración de cada alumno con el fin de que pueda volver a utilizarlo en sesiones posteriores y así no perder tiempo configurando de nuevo los equipos. No obstante, hay que avisar al usuario de que, por ejemplo, en el caso de las interfaces o las VLANs, no se guardan en el fichero de configuración, por lo que la próxima vez que continúe el laboratorio deber acordarse de que interfaces o VLANs tenía configuradas y si estaban o no levantadas.

5.8 INTEGRACIÓN CON LA APLICACIÓN DE RESERVA DE TURNOS

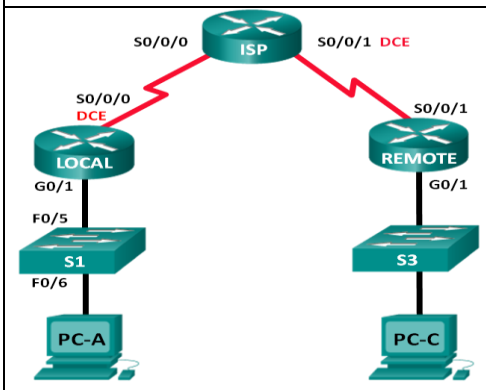
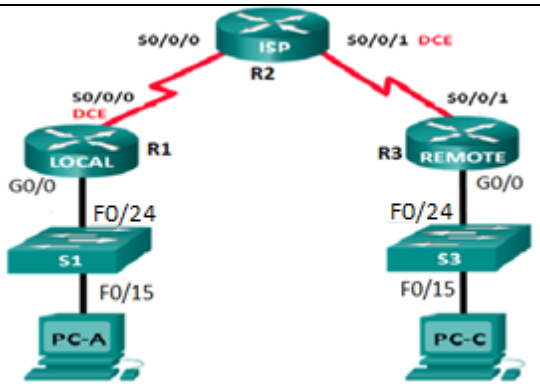
El alumno encargado de realizar la aplicación de reserva de turnos necesita conocer las diferentes topologías y laboratorios disponibles, de forma que necesita mostrar a los alumnos los nuevos laboratorios una vez editados y adaptados a las topologías físicas disponibles. Asimismo, necesita conocer las contraseñas establecidas y los parámetros

SSH para poder acceder a los diferentes equipos desde la aplicación, al igual que los eventos del Event Manager y las VLANs establecidas. Igualmente ocurre con los comandos de las configuraciones iniciales de cada equipo, los cuales necesita conocer para inyectarlos directamente mediante la aplicación tras expirar la sesión de un alumno y volver a la configuración inicial de cara al próximo alumno. También deberá conocer que ficheros de configuración guardar para que los alumnos no pierdan sus progresos.

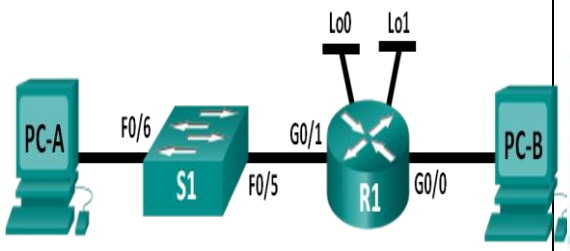
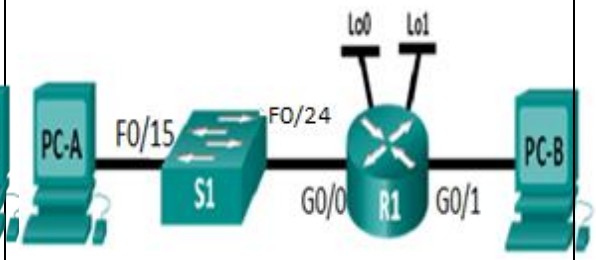
A continuación se muestran las nuevas imágenes de las topologías virtuales que se mostrarán en la aplicación web a la hora de previsualizar cada ejercicio por los alumnos. Estas topologías han variado para adaptarse a la topología física del laboratorio, por lo que los enunciados se han visto modificados para que, obviamente, también se adapten a estos cambios, la mayoría de ellos en las interfaces y en el nombrado de algunos equipos. De igual forma, a través del enunciado, se insta a los alumnos a seguir las interfaces dadas en los mismos y no borrar ni modificar las VLANs 11, 22 y 33 configuradas previamente por el administrador. Al no tener los alumnos permisos administrativos, no podrán modificar las contraseñas globales ni crear nuevas para la línea SSH ni tampoco eliminar los usuarios de administración del laboratorio o los eventos del Event Manager.

Módulo 1, "Introduction to networks":

- Ejercicio 8.3.2.7 Prueba de conectividad de red con ping y traceroute.

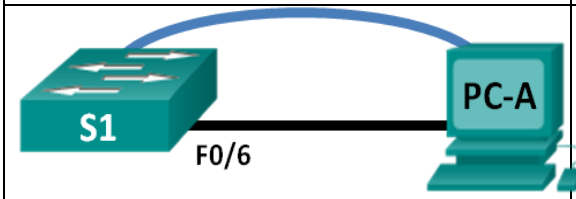
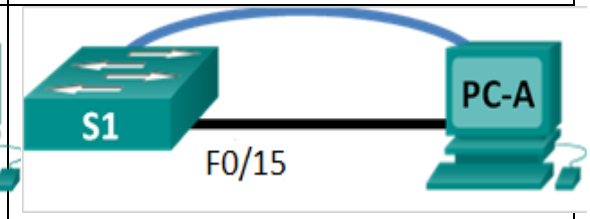
Imagen Original	Imagen Nueva
	

- Ejercicio 9.2.1.3 Diseño e implementación de un esquema de direccionamiento IPv4 dividido en subredes.

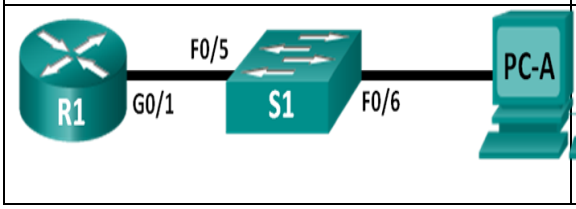
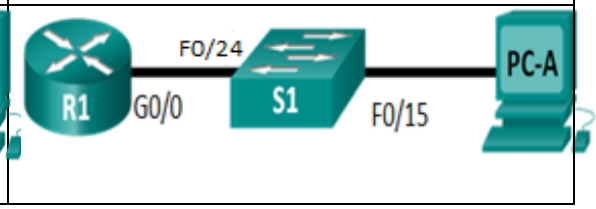
Imagen Original	Imagen Nueva
	

Módulo 2, "Routing and Switching essentials":

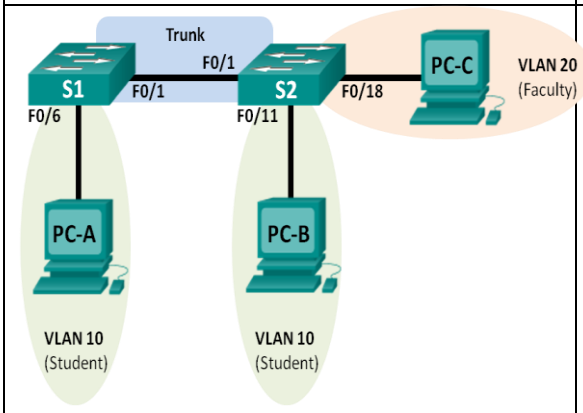
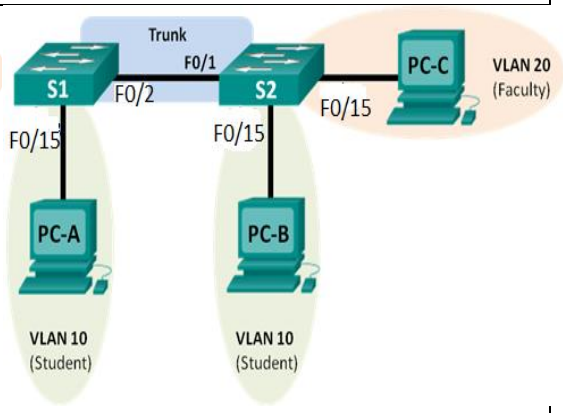
- Ejercicio 2.1.1.6 Configuración de los parámetros básicos de un switch.

Imagen Original	Imagen Nueva
	

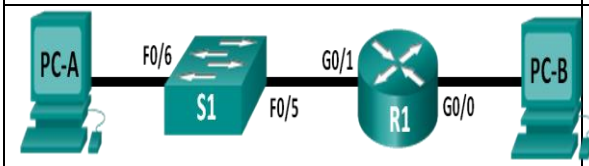
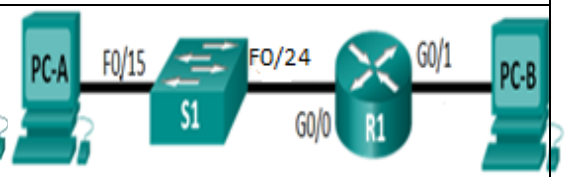
- Ejercicio 2.2.4.11 Configuración de características de seguridad de switch.

Imagen Original	Imagen Nueva
	

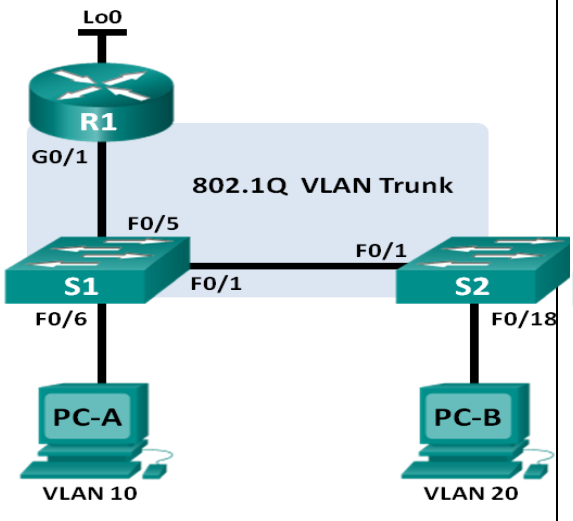
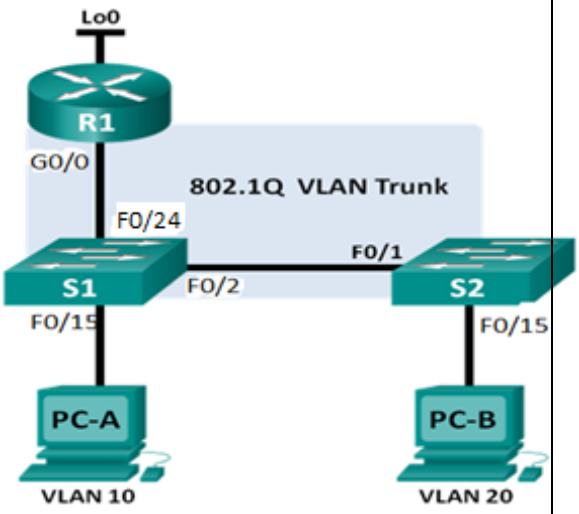
- Ejercicio 3.2.2.5 Configuración de redes VLAN y enlaces troncales.

Imagen Original	Imagen Nueva
	

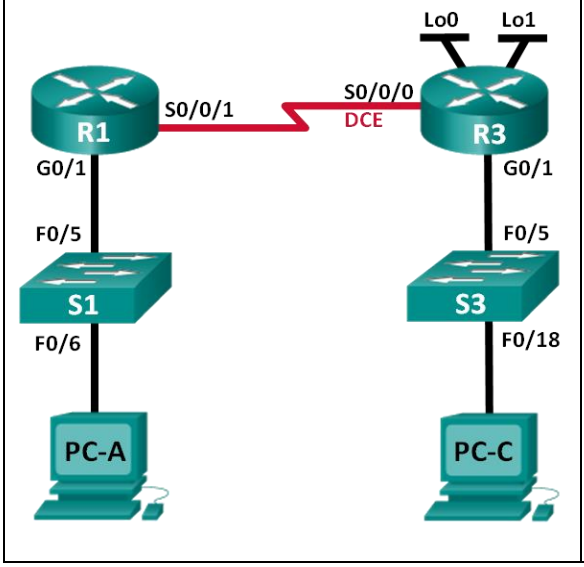
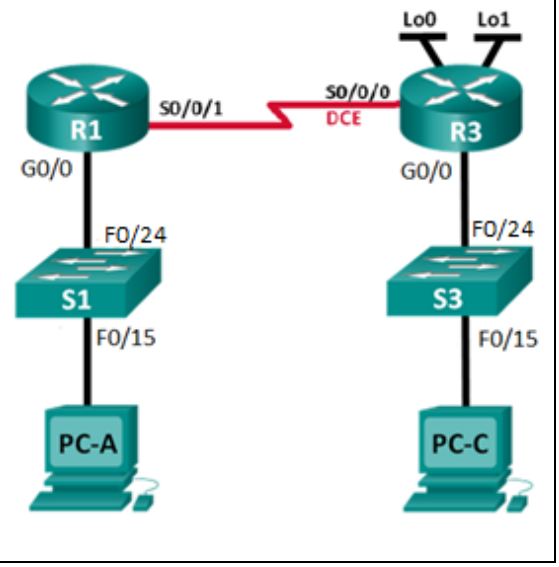
- Ejercicio 4.1.4.6 Configuración de los parámetros básicos de un router.

Imagen Original	Imagen Nueva
	

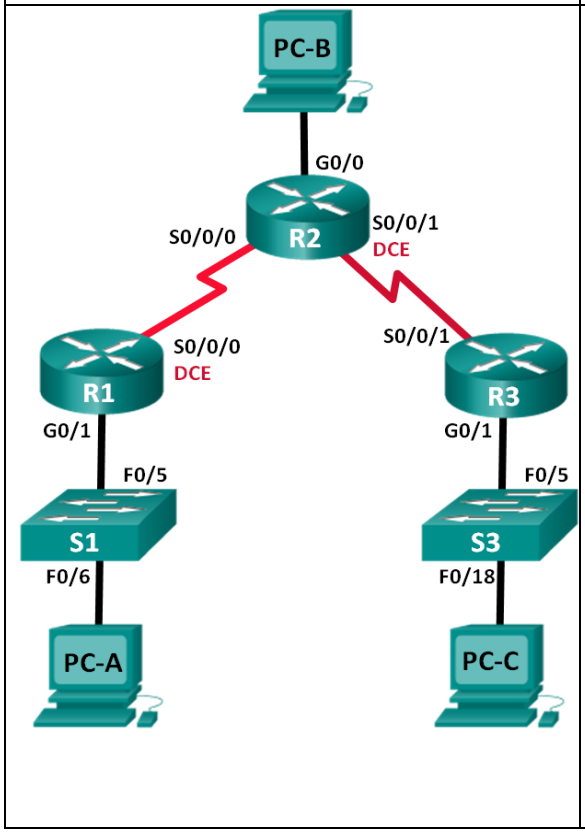
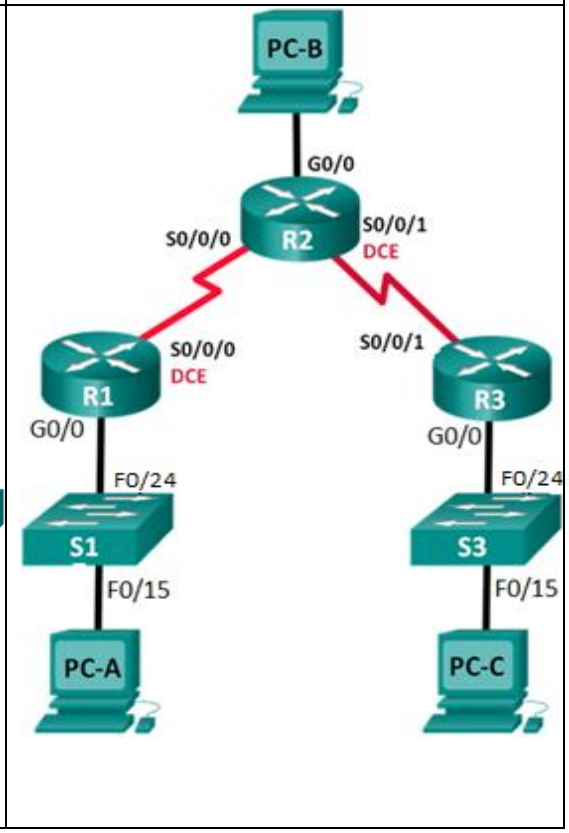
- Ejercicio 5.1.3.7 Configuración de routing entre VLAN basado en enlaces troncales 802.1Q.

Imagen Original	Imagen Nueva
	

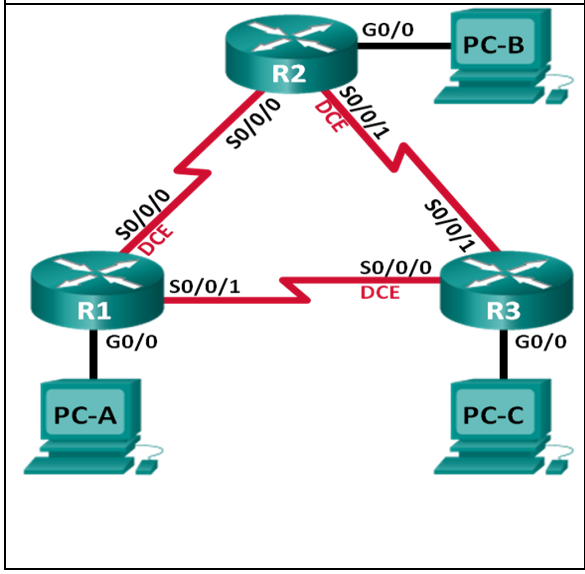
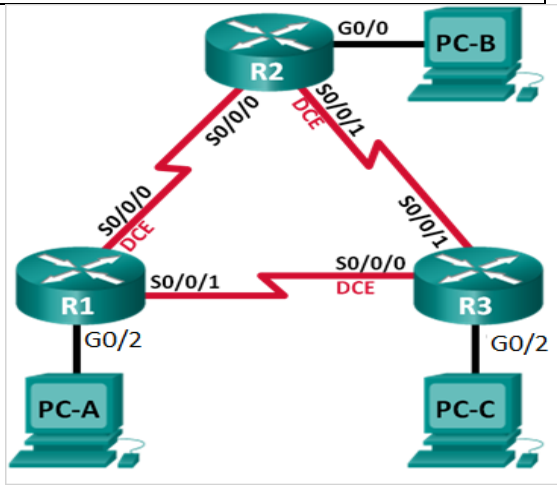
- Ejercicio 6.2.2.5 Configuración de rutas estáticas y predeterminadas IPv4.

Imagen Original	Imagen Nueva
	

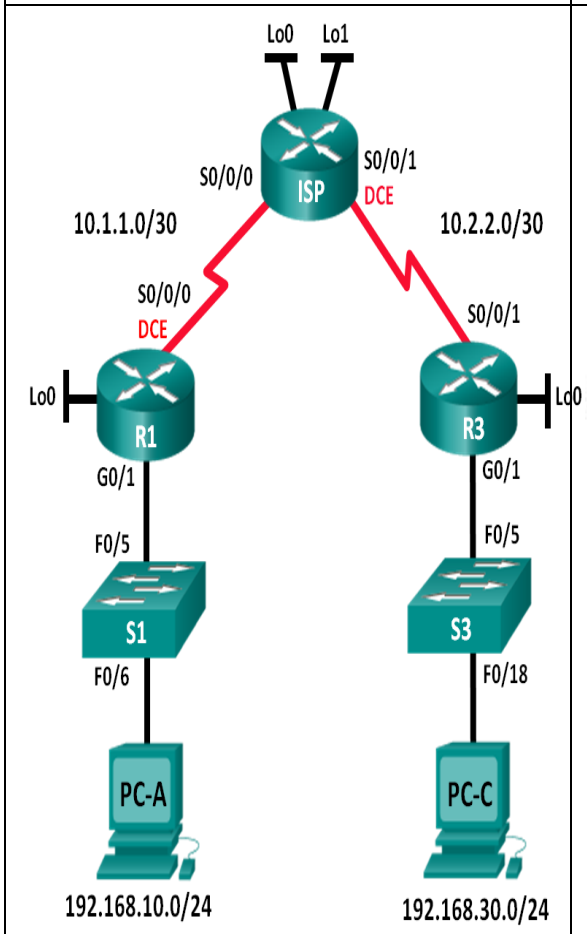
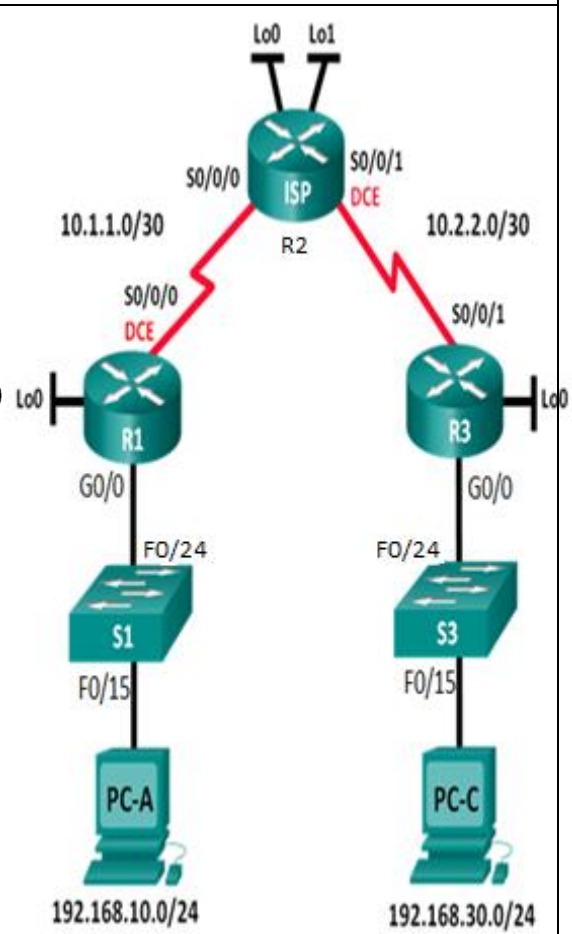
- Ejercicio 7.3.2.4 Configuración básica de RIPv2 y RIPng.

Imagen Original	Imagen Nueva
	

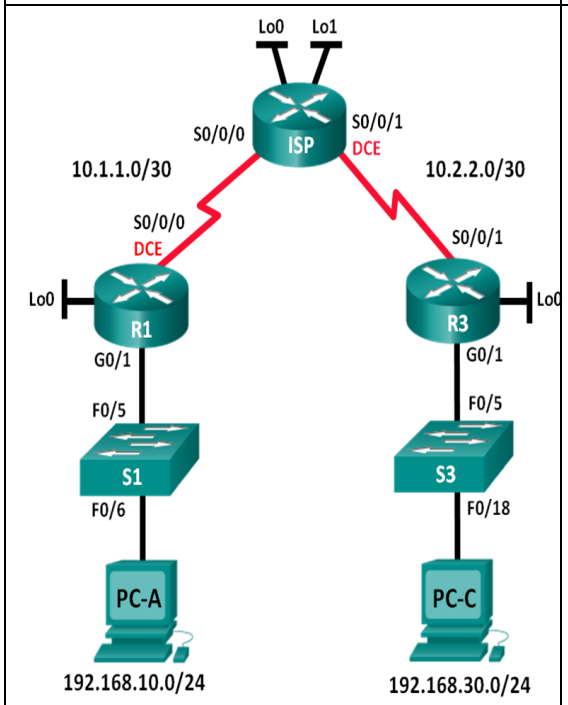
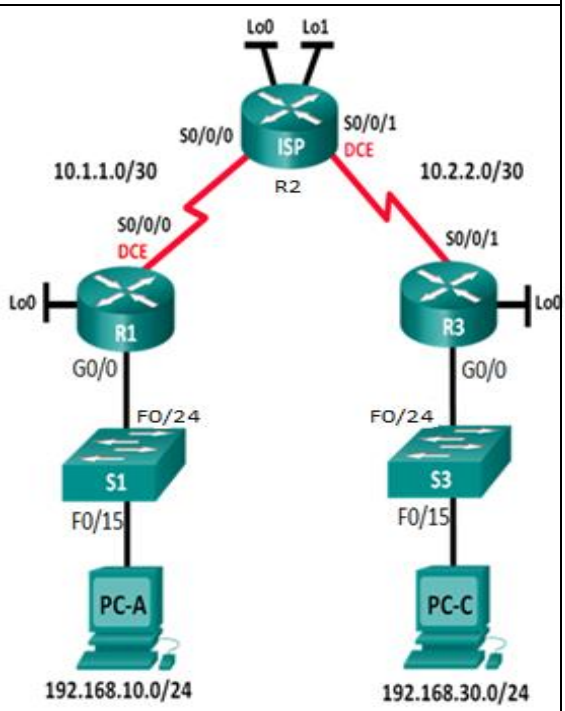
- Ejercicio 8.2.4.5 Configuración de OSPFv2 básico de área única.

Imagen Original	Imagen Nueva
	

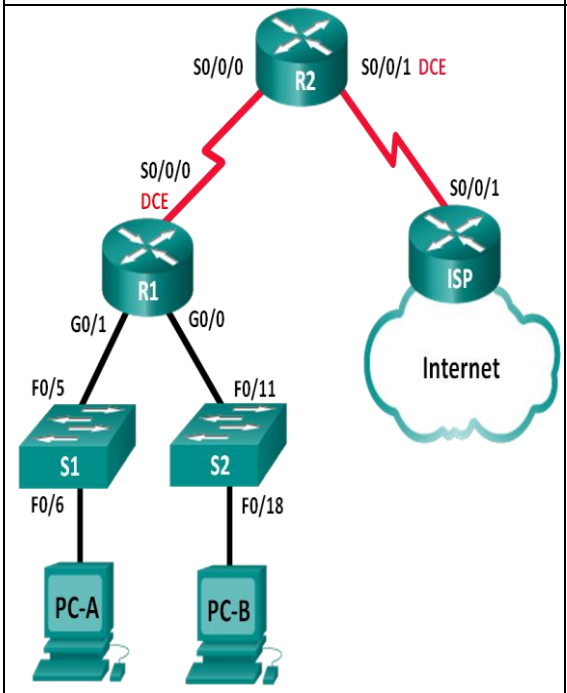
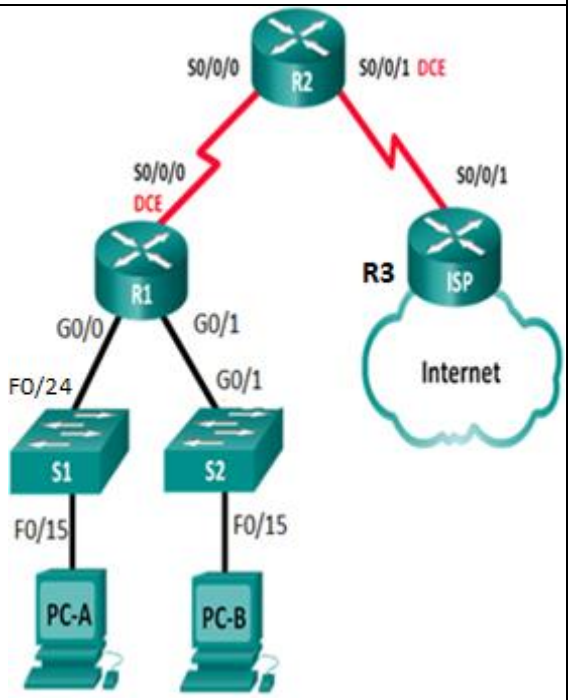
- Ejercicio 9.2.2.7 Configuración y verificación de ACL estándares.

Imagen Original	Imagen Nueva
	

- Ejercicio 9.3.2.13 Configuración y verificación de ACL extendidas.

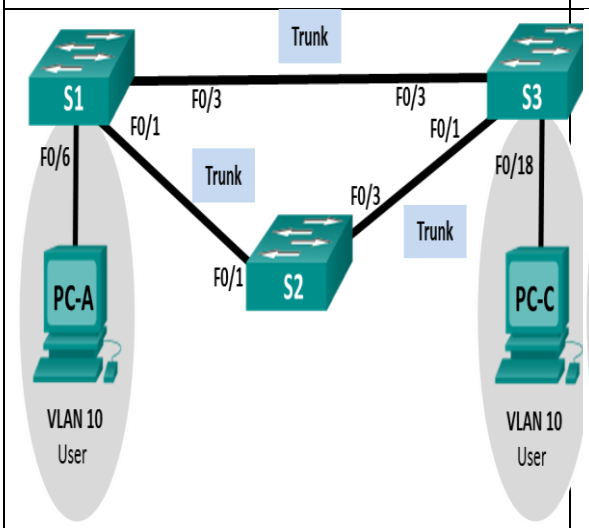
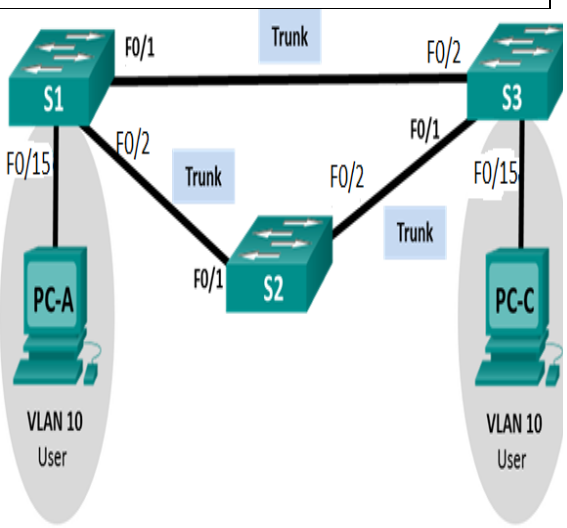
Imagen Original	Imagen Nueva
	

- Ejercicio: 10.1.2.4 Configuración de DHCPv4 básico en un router.

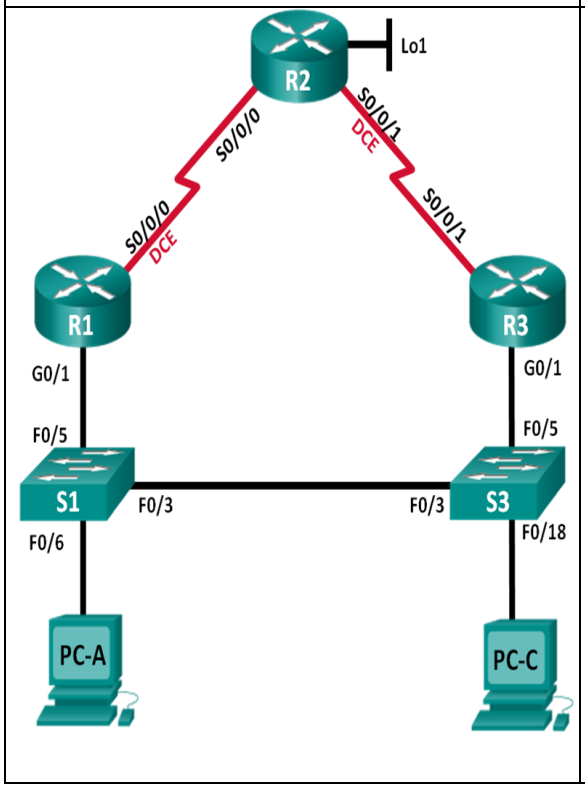
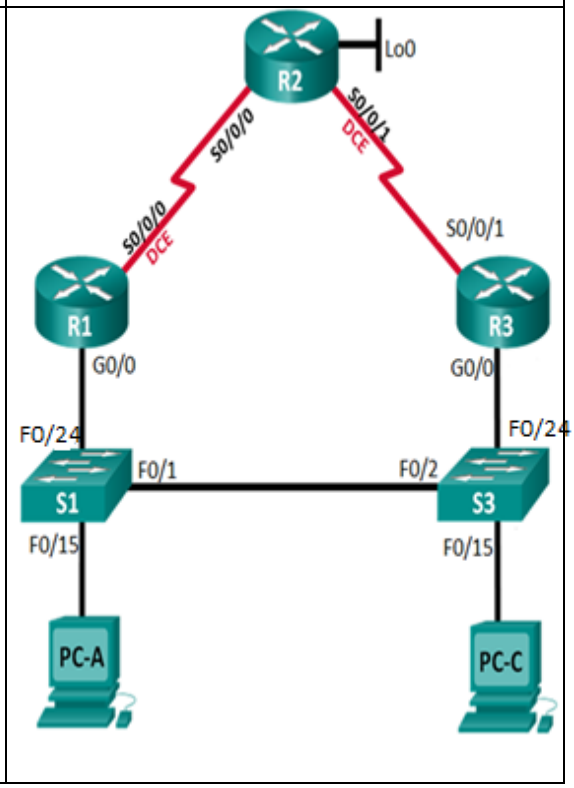
Imagen Original	Imagen Nueva
	

Módulo 3, “Scalling networks”:

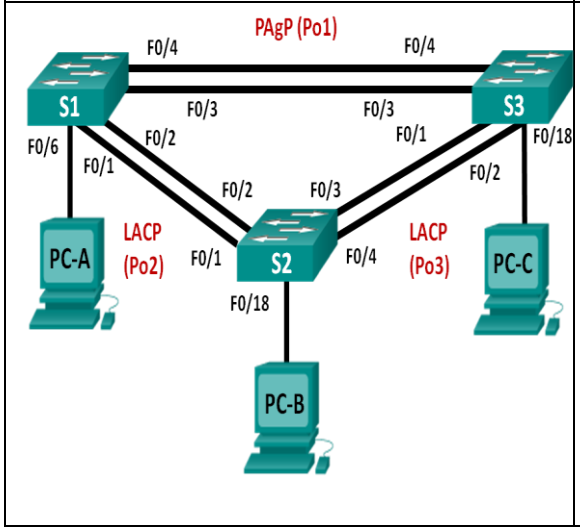
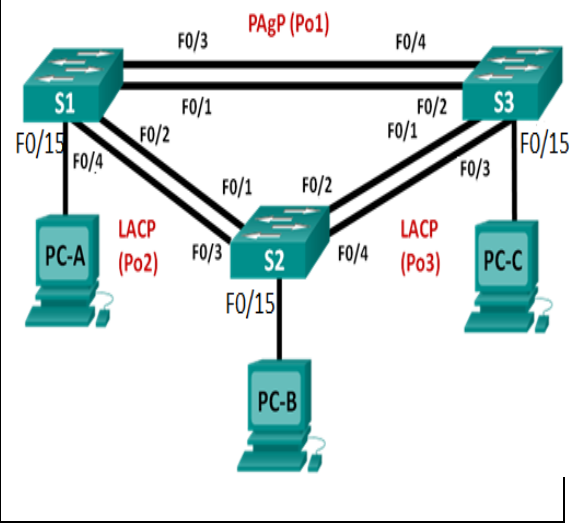
- Ejercicio 2.3.2.3 Configuración de PVST+ rápido, PortFast y protección BPDU.

Imagen Original	Imagen Nueva
	

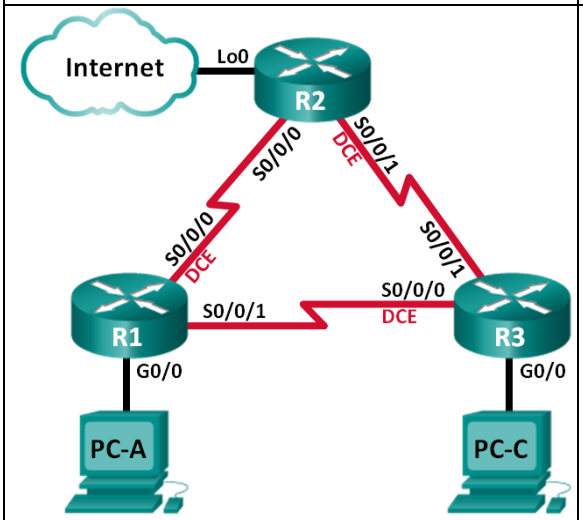
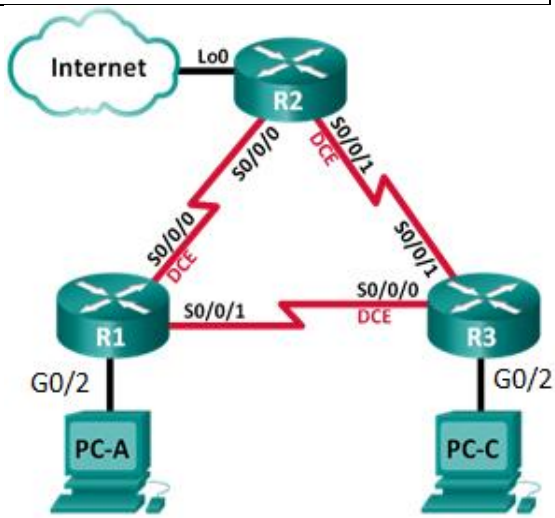
- Ejercicio 2.4.3.4 Configuración de HSRP y GLBP.

Imagen Original	Imagen Nueva
	

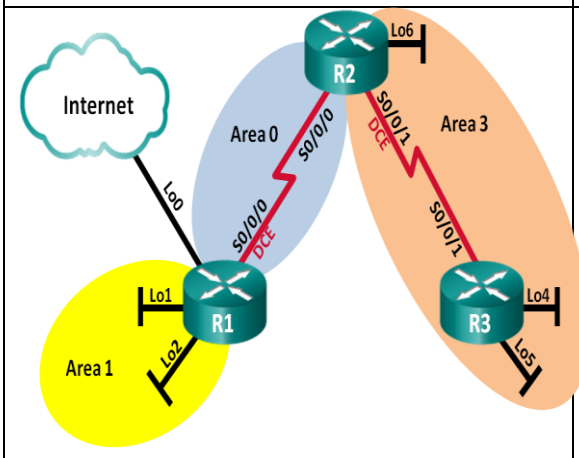
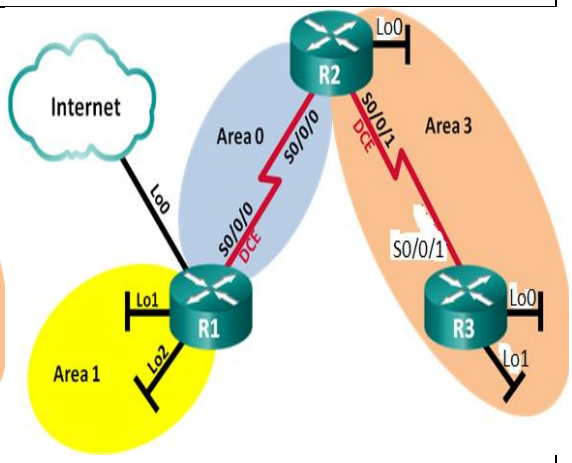
- Ejercicio 3.2.1.4 Configuración de EtherChannel.

Imagen Original	Imagen Nueva
	

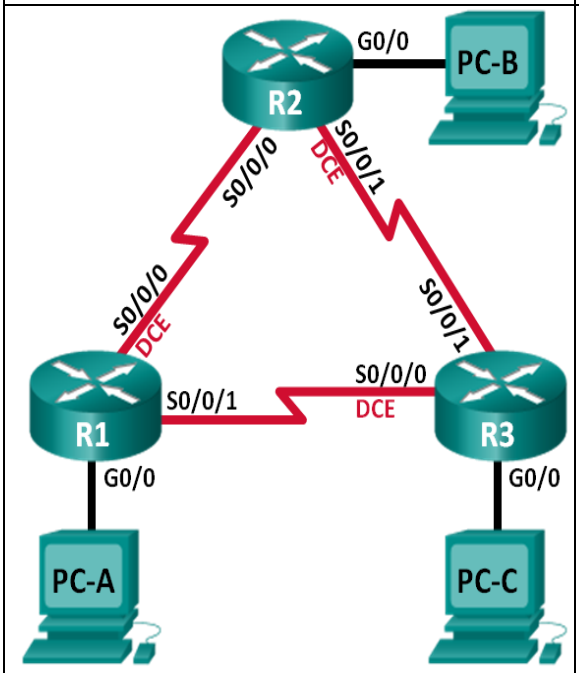
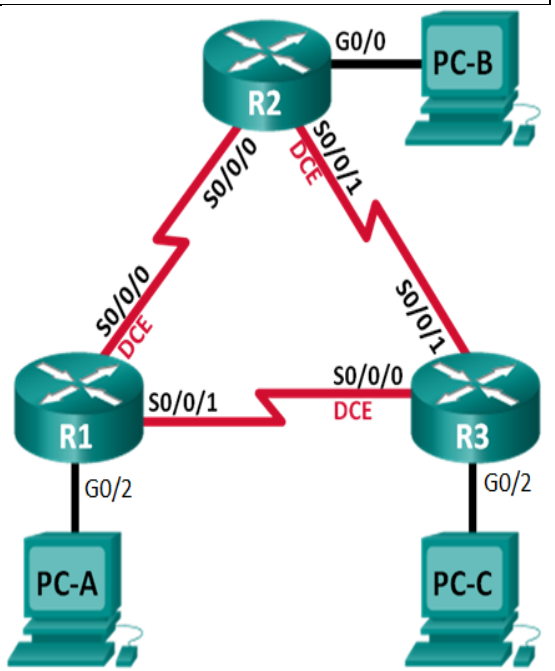
- Ejercicio 5.1.5.8 Configuración de las características avanzadas de OSPFv2.

Imagen Original	Imagen Nueva
	

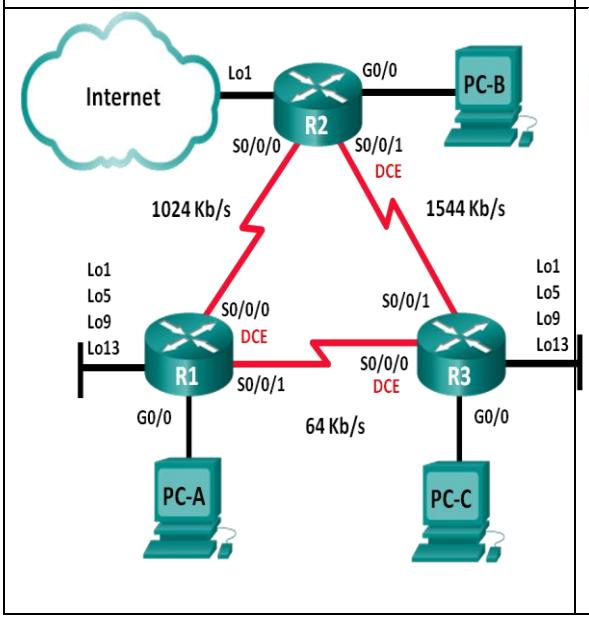
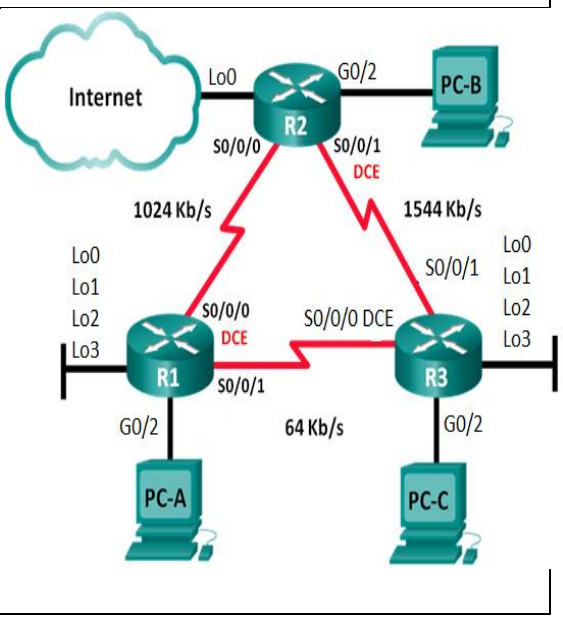
- Ejercicio 6.2.3.8 Configuración de OSPFv2 multiárea.

Imagen Original	Imagen Nueva
	

- Ejercicio 7.2.2.5 Configuración de EIGRP básico para IPv4.

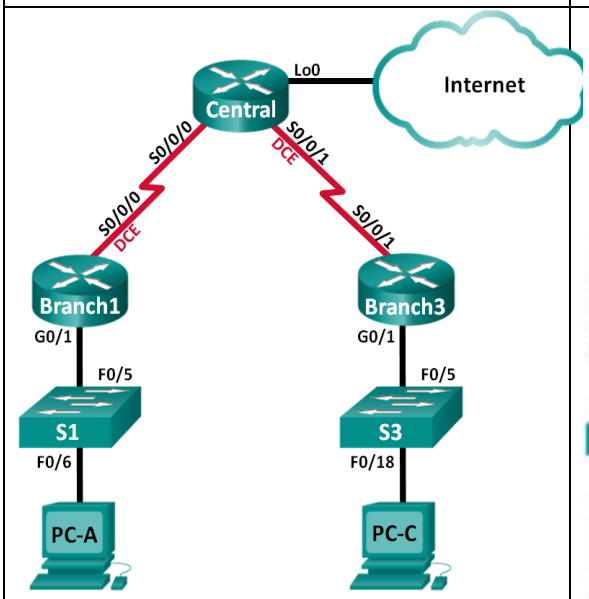
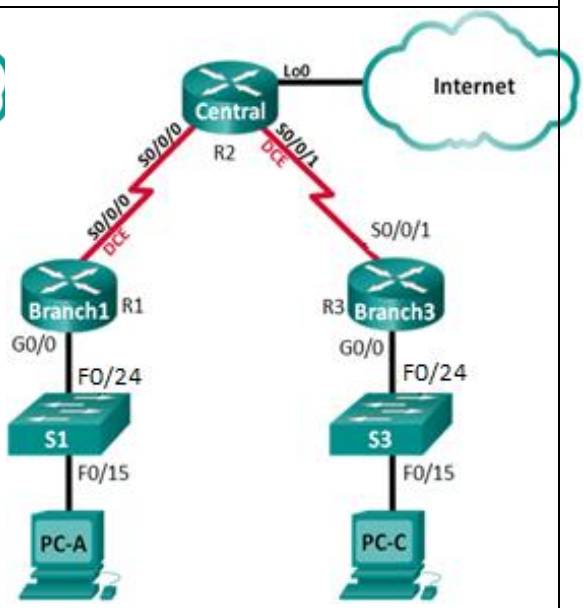
Imagen Original	Imagen Nueva
	

- Ejercicio 8.1.5.5 Configuración de EIGRP avanzado para admitir características de IPv4.

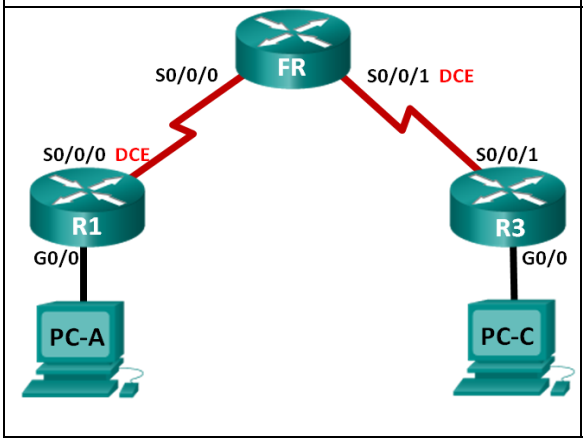
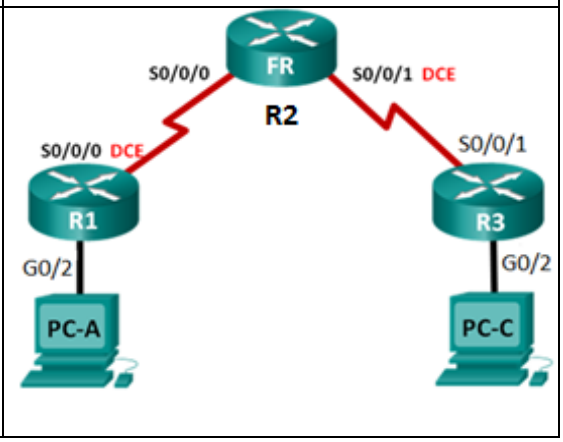
Imagen Original	Imagen Nueva
	

Módulo 4, “Connecting networks”:

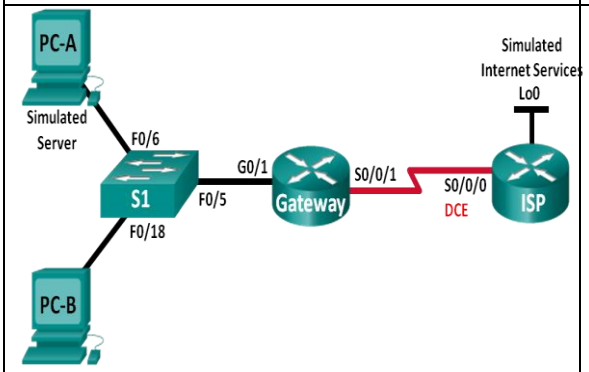
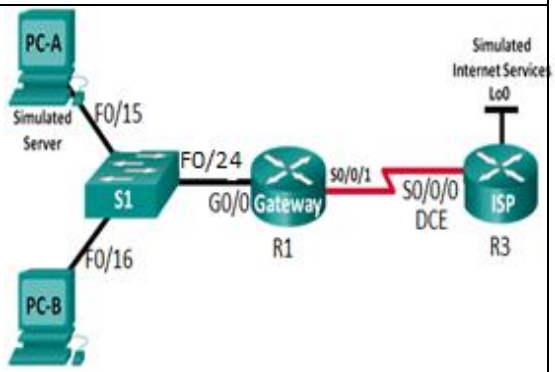
- Ejercicio 3.3.2.8 Configuración de PPP básico con autenticación.

Imagen Original	Imagen Nueva
	

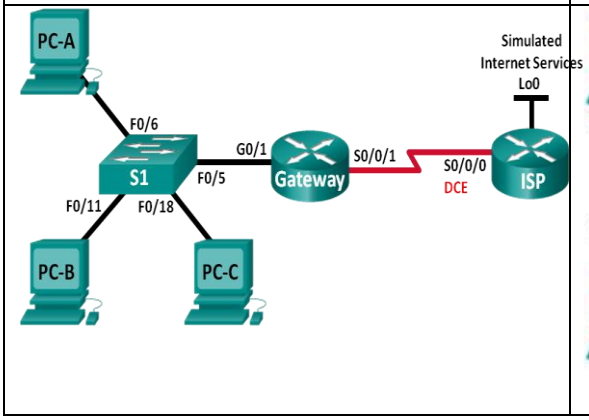
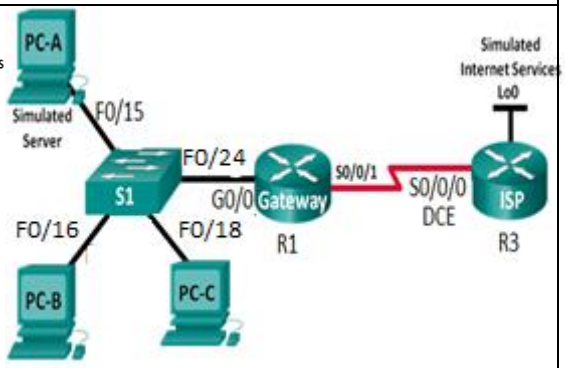
- Ejercicio 4.2.2.7 Configuración de Frame Relay y subinterfaces.

Imagen Original	Imagen Nueva
	

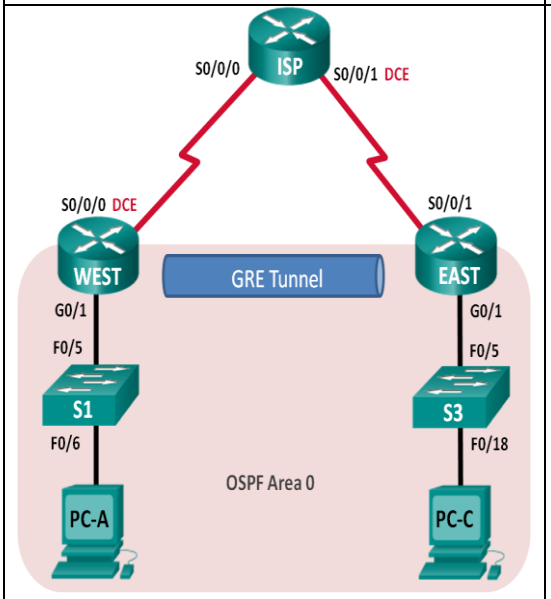
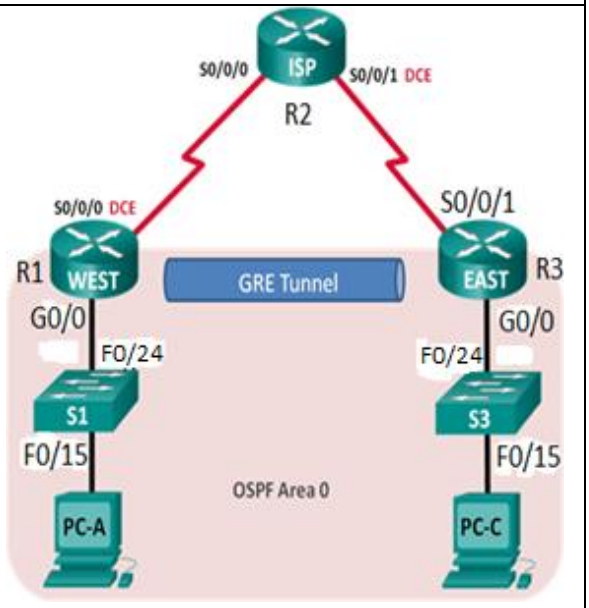
- Ejercicio 5.2.2.6 Configuración de NAT dinámica y estática.

Imagen Original	Imagen Nueva
	

- Ejercicio 5.2.3.7 Configuración de la traducción de la dirección del puerto (PAT).

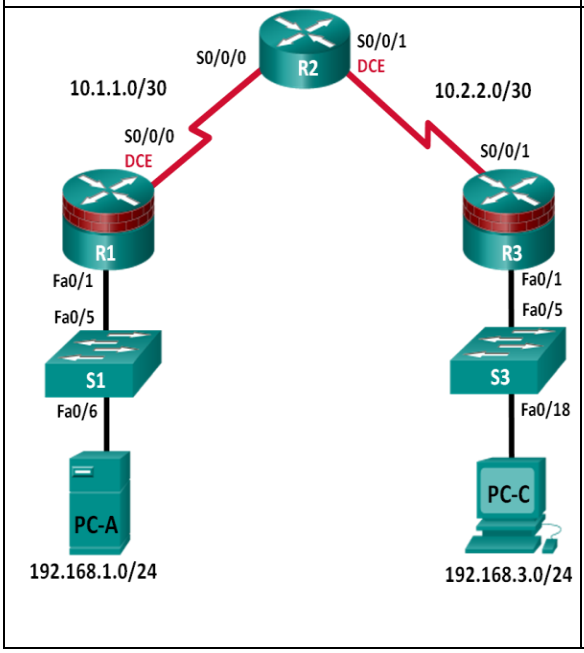
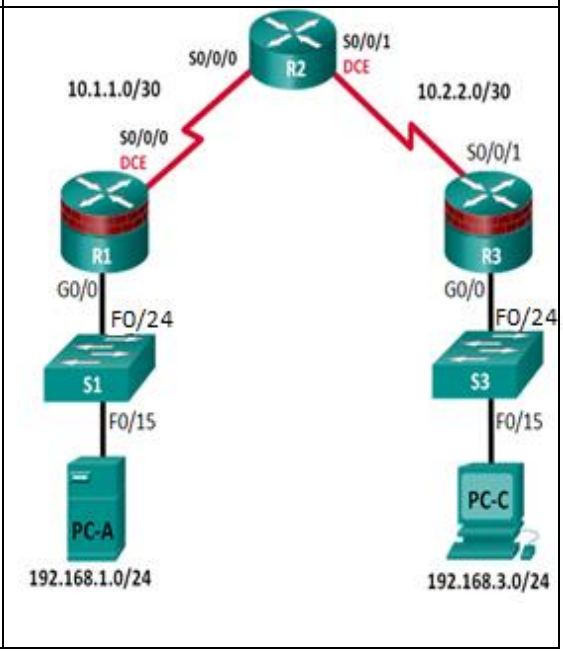
Imagen Original	Imagen Nueva
	

- Ejercicio 7.2.2.5 Configuración de un túnel VPN GRE de punto a punto.

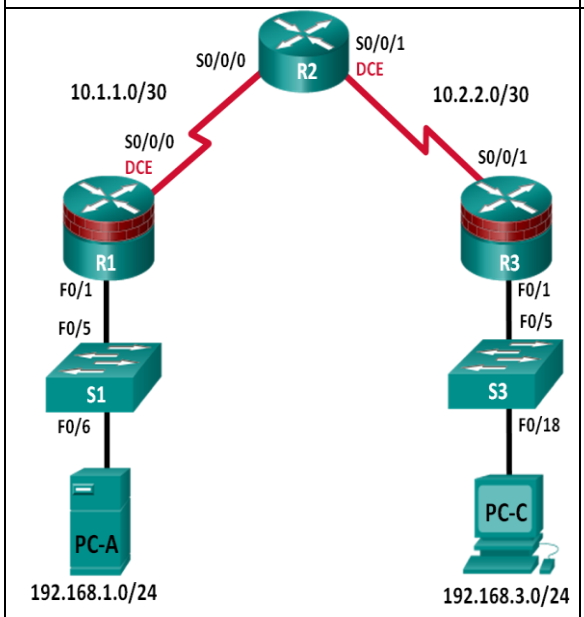
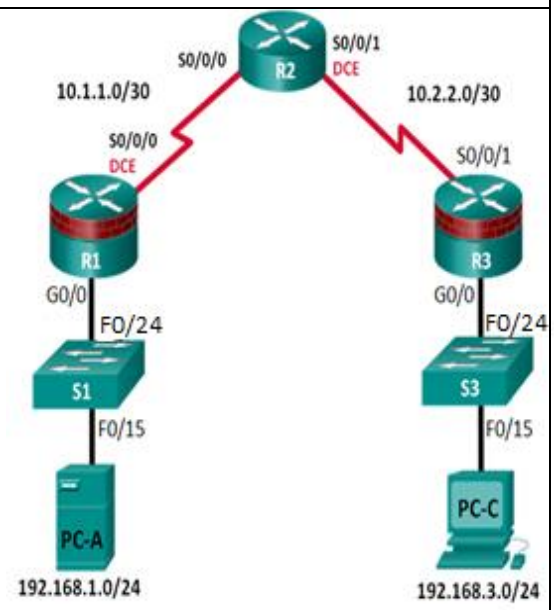
Imagen Original	Imagen Nueva
	

CCNA Security:

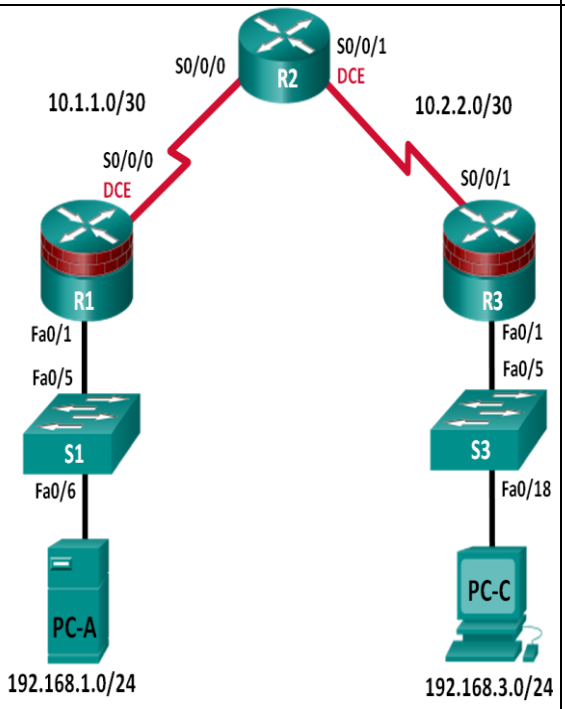
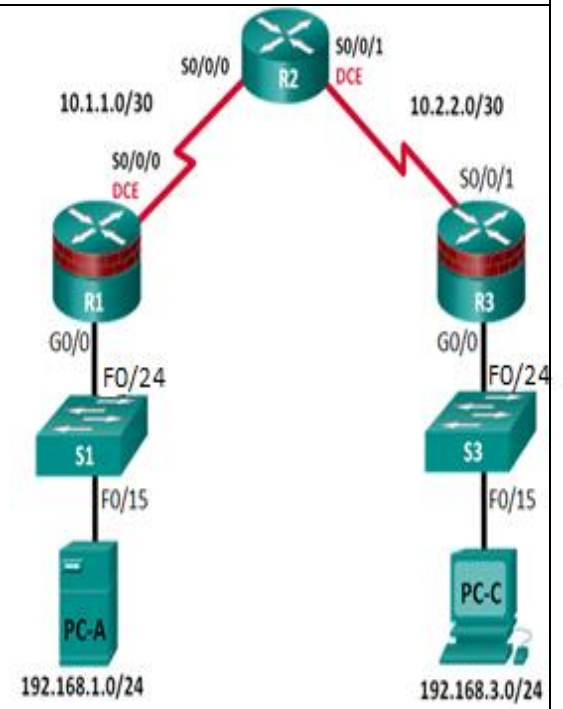
- Ejercicio 2.5.1.1 Securización del router para acceso administrativo.

Imagen Original	Imagen Nueva
	

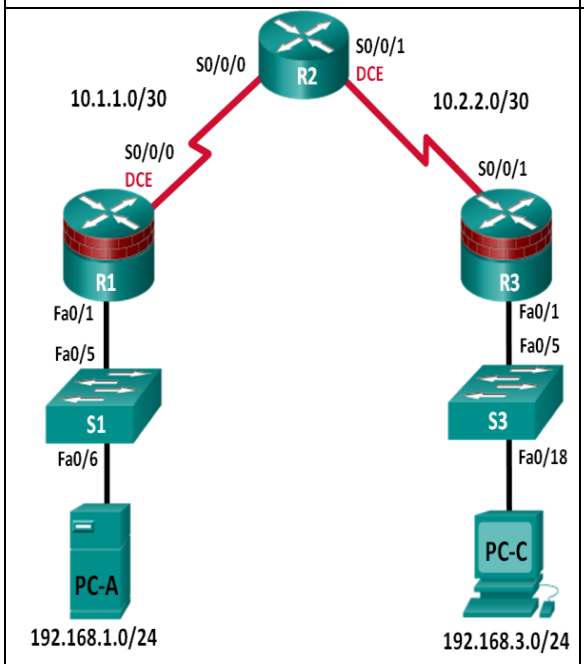
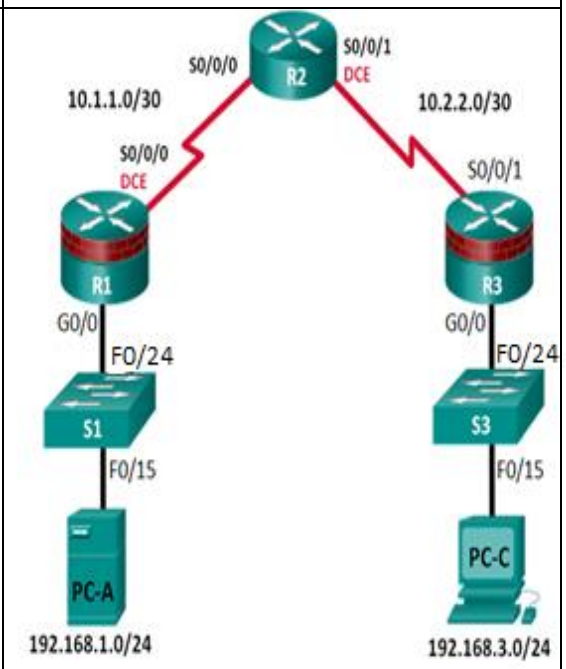
- Ejercicio 3.6.1.1 Securización de acceso administrativo usando AAA y servidor Radius.

Imagen Original	Imagen Nueva
	

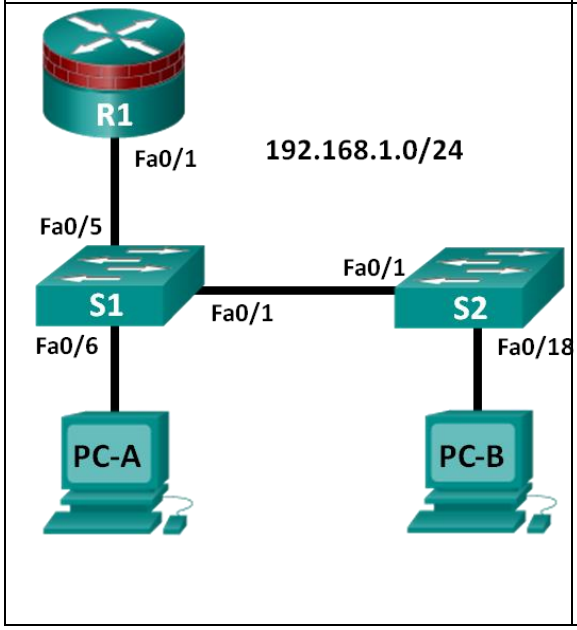
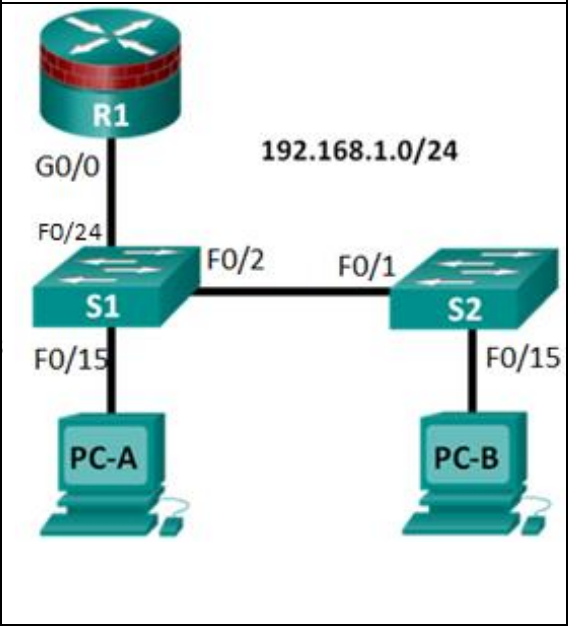
- Ejercicio 4.4.1.1 Configurar políticas zonales mediante Firewalls.

Imagen Original	Imagen Nueva
	

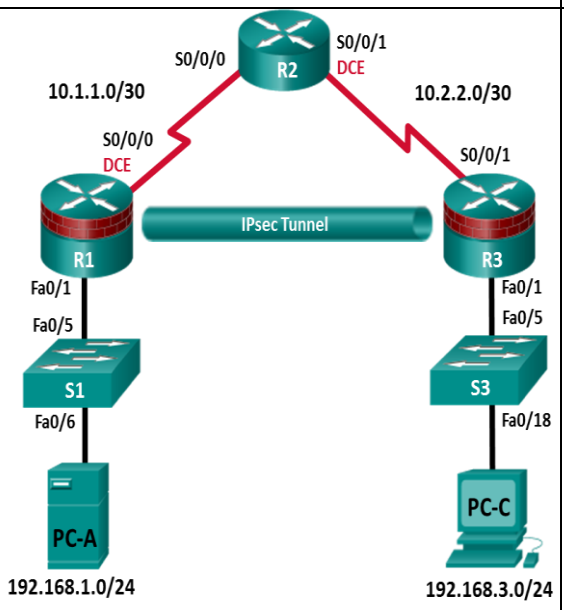
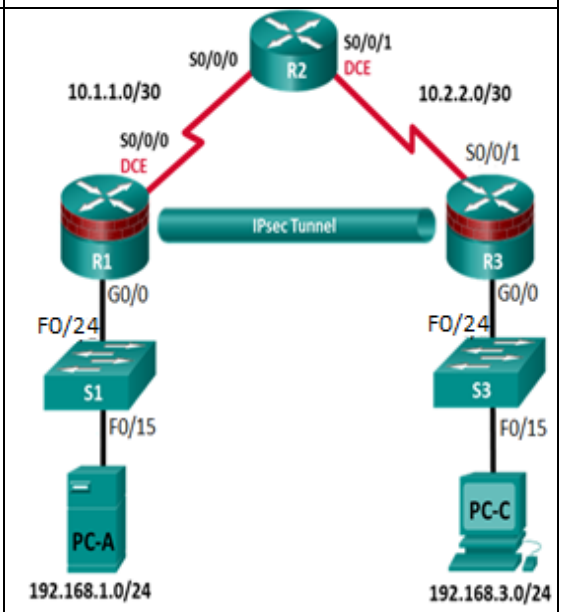
- Ejercicio 5.5.1.1 Configurar un sistema de prevención de intrusiones (IPS) usando CLI y CCP.

Imagen Original	Imagen Nueva
	

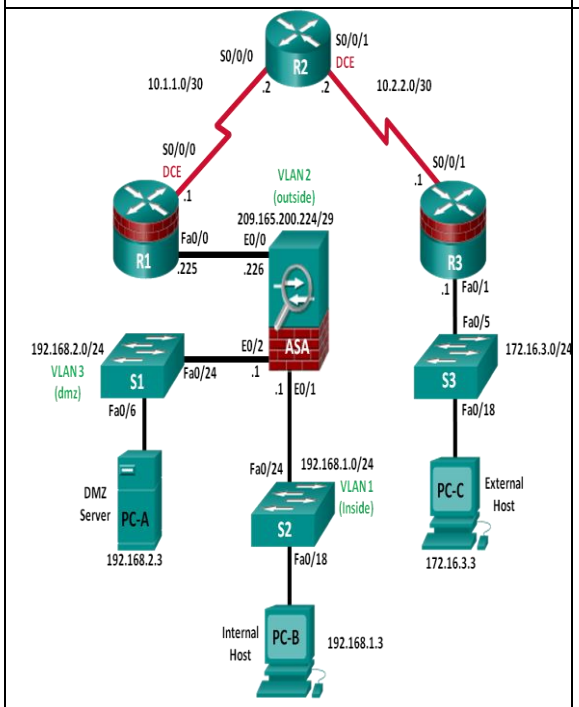
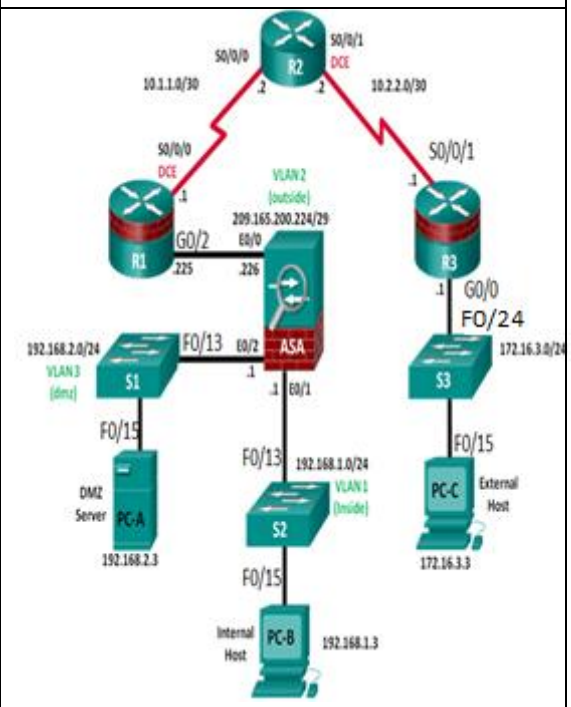
- Ejercicio 6.5.1.1 Asegurar la segunda capa de los switches.

Imagen Original	Imagen Nueva
	

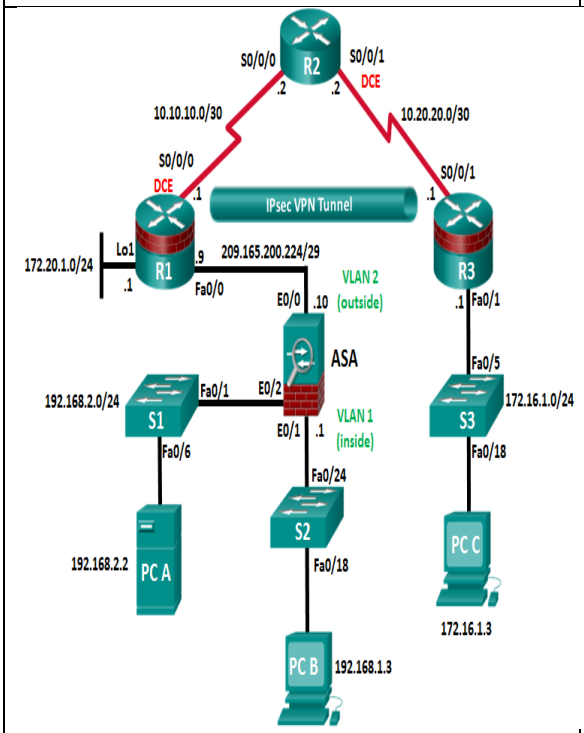
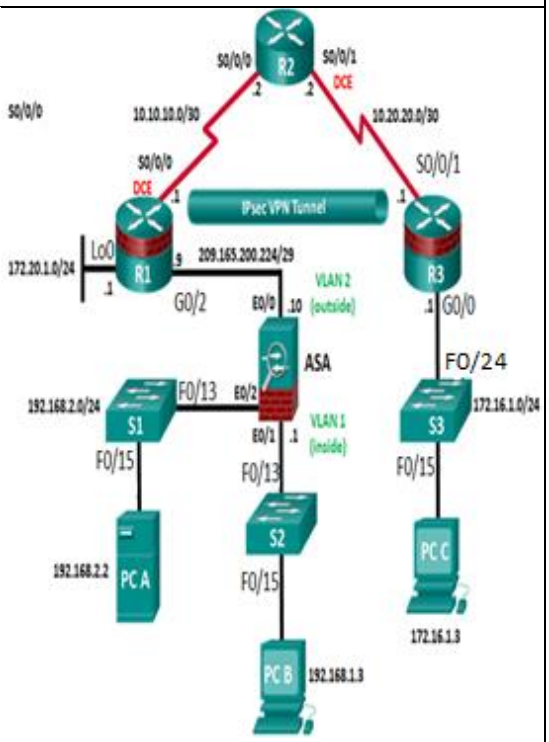
- Ejercicio 8.7.1.1 Configurar una Site-to-Site VPN usando Cisco IOS y CCP.

Imagen Original	Imagen Nueva
	

- Ejercicio 9.4.1.1 Configurar parámetros básico para un ASA y un Firewall usando CLI.

Imagen Original	Imagen Nueva
	

- Ejercicio 10.8.1.1 CCNA Security Laboratorio

Imagen Original	Imagen Nueva
	

6. RESULTADOS

La lista de tareas se ha seguido tal y como se estipuló a principio del trabajo en su plan, aunque algunas hayan tomado mayor tiempo del requerido o se hayan paralelizado algunas con el fin de adelantar su realización.

Nombre de la tarea	**Horas previstas dedicadas**
Elaboración del plan de trabajo a seguir durante el Trabajo de Fin de Grado	4 horas
Instalar el kit de laboratorio físico	10 horas
Adquirir conocimientos generales de los equipos del laboratorio (Routers, Switches, ASA's (Firewalls))	20 horas
Adquirir nuevos conocimientos de Apache Tomcat, Java (JSF, JavaServer Faces; JPA, Java Persistence API), bases de datos y de CCNA R&S y CCNA-S para la posterior configuración de los escenarios virtuales	20 horas
Diseño de los escenarios físicos (Documentación ejercicios, laboratorio físico)	25 horas
Diseño de los escenarios virtuales (Ficheros .pkt, realizar configuraciones individuales de las topologías)	50 horas
Comprobación de la adecuación de las topologías soportadas	20 horas
Configuración automatizada de los equipos físicos en base a una topología • Configuración de los apartados de seguridad de cada topología • Configuración del Access Server • Realizar las configuraciones automáticas iniciales de cada topología • Añadir el trabajo a los proyectos dinámicos de JSF y JPA	95 horas 25 horas 10 horas 30horas 30horas
Realización del guardado automático de las configuraciones previas y posibles *backups* o copias de seguridad que necesiten los usuarios	50 horas
Elaboración de la documentación del proyecto y de la memoria del Trabajo de Fin de Grado	25 horas
Preparación de la defensa del Trabajo de Fin de Grado	5 horas

Cómputo total aproximado del trabajo	324 horas

Al no haberse introducido ninguna modificación ni en la lista de tareas, el Diagrama de Gantt que se ha seguido es exactamente el mismo en cuestión de tiempo y de tareas.

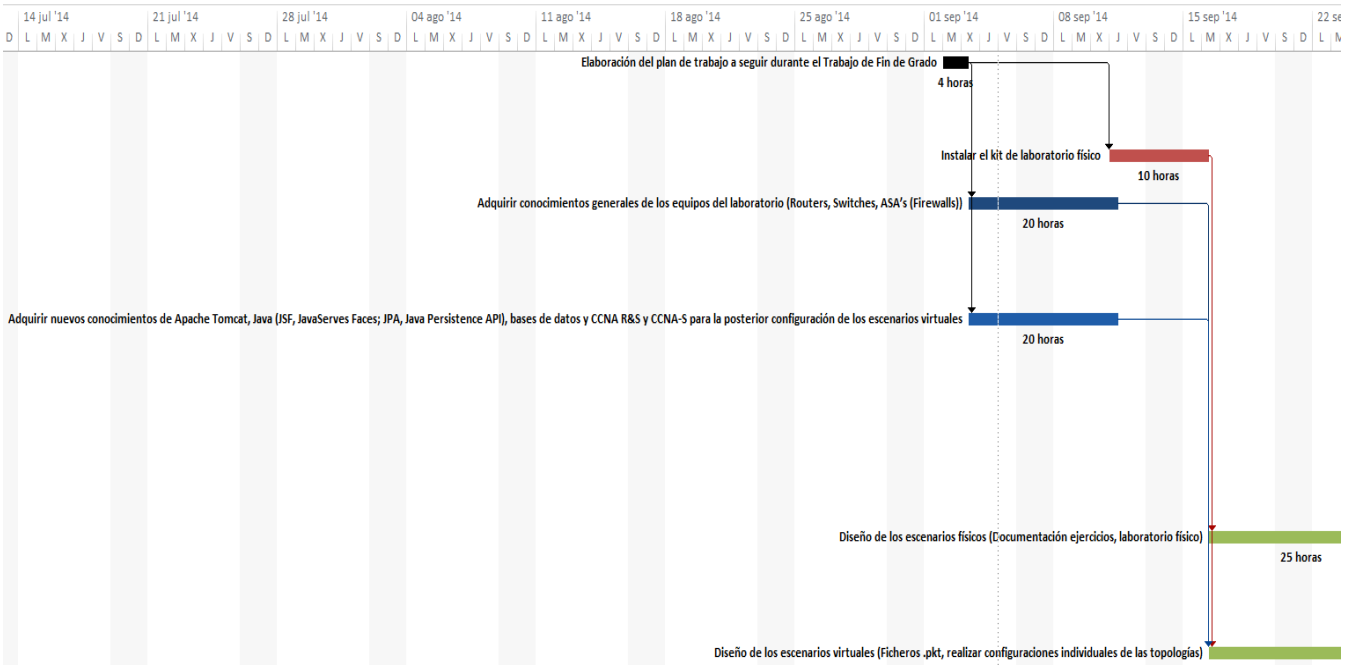


Diagrama de Gantt - 1

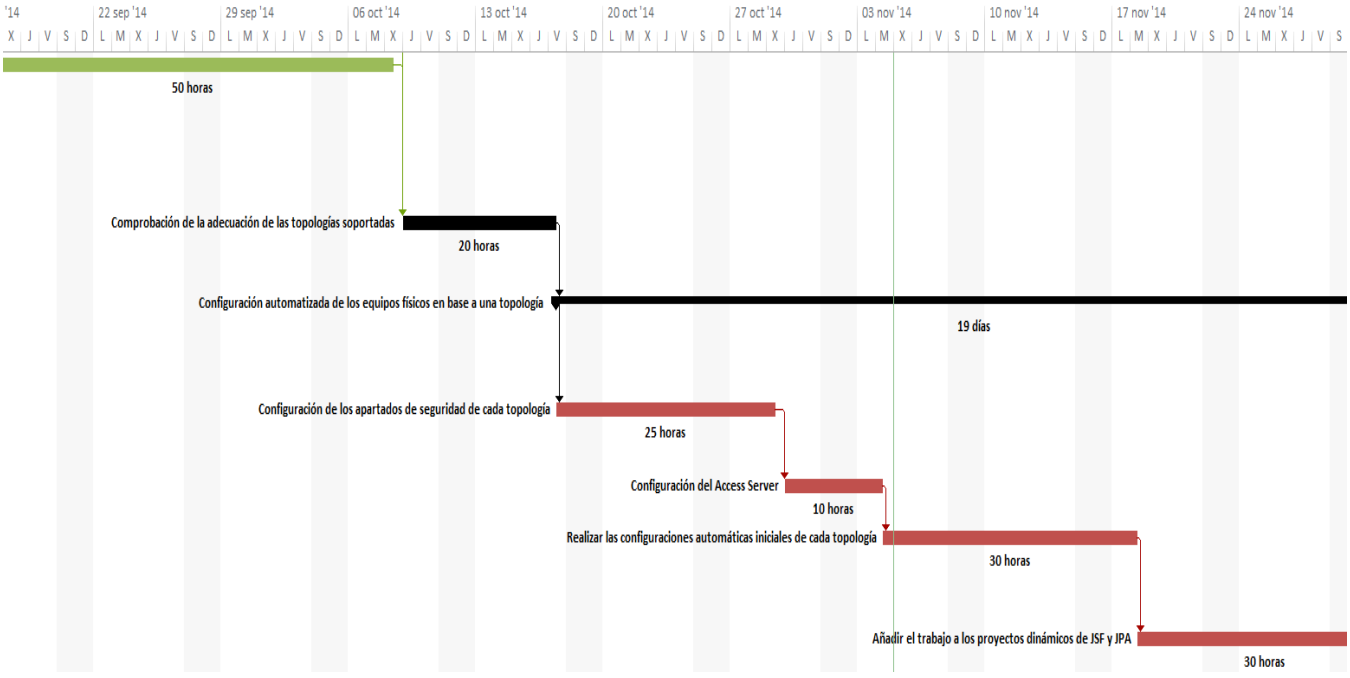


Diagrama de Gantt – 2

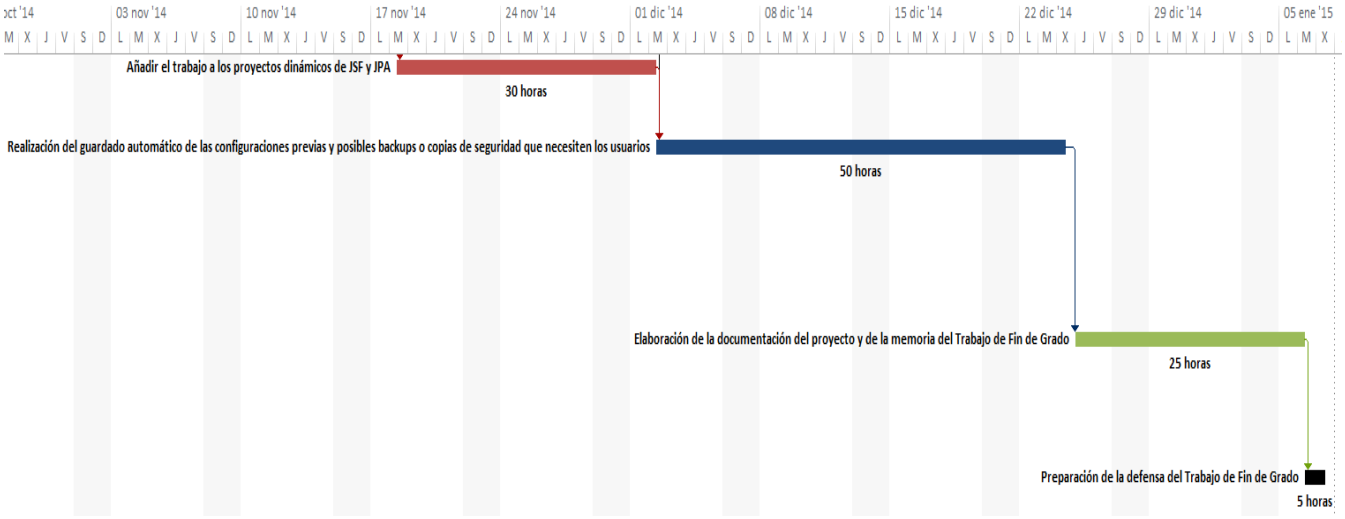
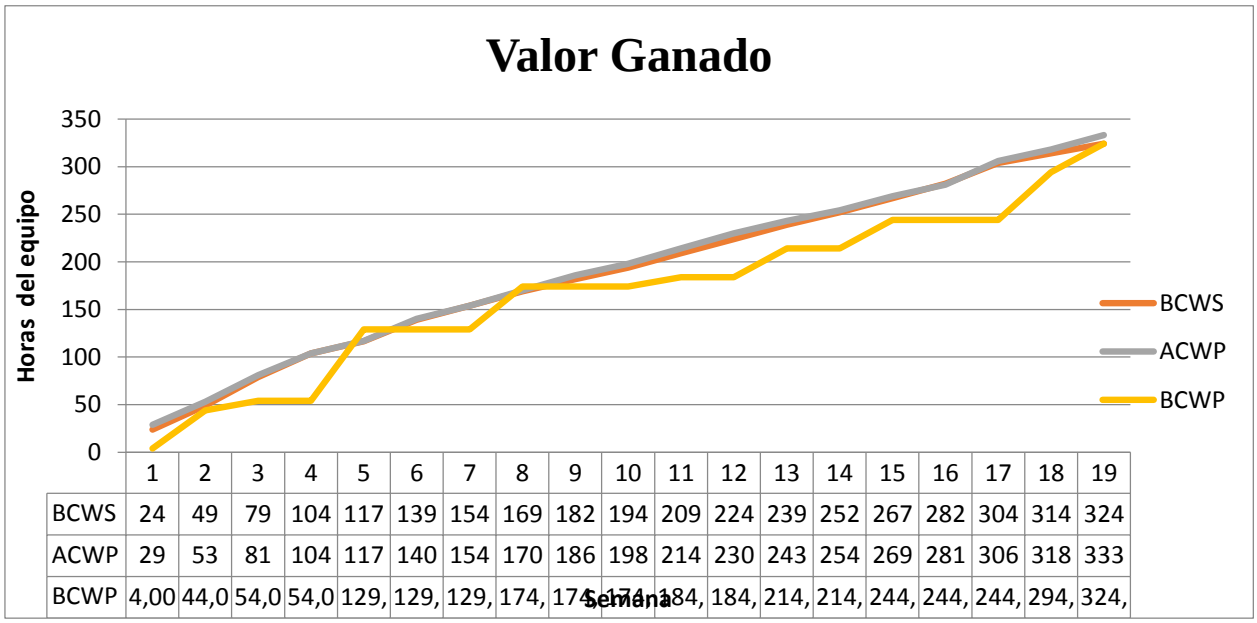


Diagrama de Gantt – 3

En la siguiente gráfica de valor ganado, apreciamos que las tareas se cumplieron prácticamente según lo estipulado hasta la semana 8. No obstante, a partir de ese punto las tareas se empezaron a alargar y retrasar, siendo necesario trabajar al final más horas que las planificadas inicialmente, 333 reales por las 324 planificadas.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
BCWS	24	49	79	104	117	139	154	169	182	194	209	224	239	252	267	282	304	314	324
ACWP	29	53	81	104	117	140	154	170	186	198	214	230	243	254	269	281	306	318	333
BCWP	4,00	44,0	54,0	54,0	129,	129,	129,	174,	174,	174,	184,	184,	214,	214,	244,	244,	244,	294,	324,

A lo largo del trabajo nos hemos encontrado con algunos problemas a la hora de llevar a cabo las tareas, como por ejemplo la disponibilidad del laboratorio para poder acudir a montar los kits o el hecho de depender de las fechas en las que los equipos llegarían a la facultad mediante mensajería, lo que ha hecho que las tareas se retrasaran un poco, como se aprecia en la gráfica de valor ganado.

A continuación se muestra el orden que se ha seguido para la realización del trabajo de una forma más intuitiva:

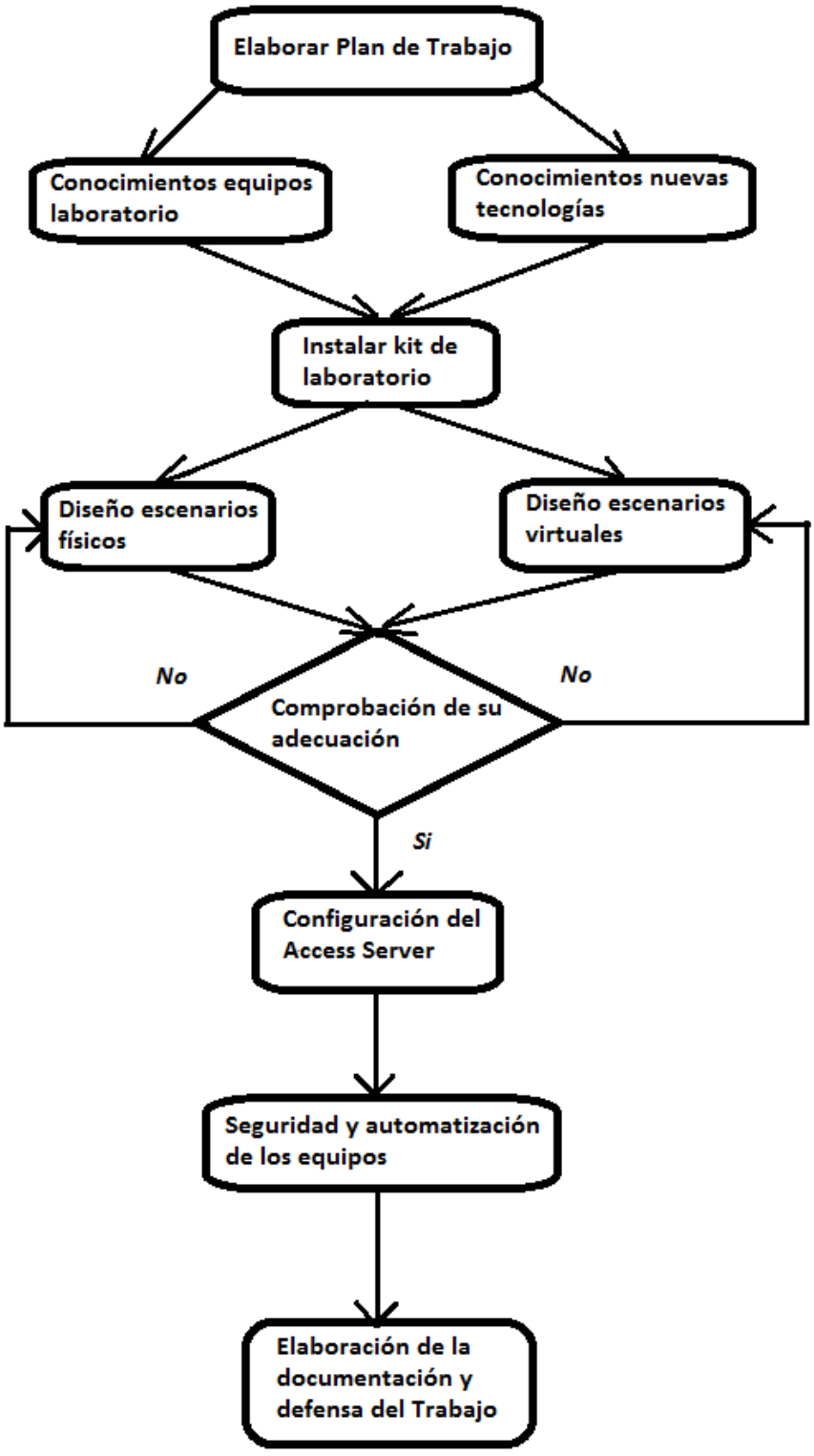


Diagrama de flujo del proyecto

7. CONCLUSIONES Y OPINIÓN PERSONAL

Estoy bastante satisfecho con la realización de este Trabajo de Fin de Grado por varias razones. En primer lugar, destacaría el tema sobre el que lo he realizado, pues desde que cursé la asignatura de "Tecnologías de Red CISCO: CCNA" me había interesado más sobre este tema y las redes en general. En segundo lugar, la idea de realizar un laboratorio remoto también me atrajo mucho a la hora de escoger Trabajo de Fin de Grado, al igual que haber conocido a mi tutor previamente en asignaturas como la anteriormente mencionada o "Redes de Computadores".

Entre los objetivos técnicos conseguidos cabe destacar:

- Revisión y elección de los ejercicios de los cursos CISCO CCNA Routing & Switching y CCNA Security que puedan adaptarse a las características del laboratorio físico.
- Modificar los enunciados originales para que se adapten a la nueva topología física y el alumno no tenga problemas para seguir los ejercicios.
- Instalación del kit de laboratorio físico (routers, switches y firewalls) y su cableado de red con el fin de emular las configuraciones virtuales que se encuentran en la currícula de los cursos CISCO CCNA Routing & Switching y CCNA Security.
- Establecer un único escenario físico compatible con todos a los que se desea dar soporte, teniendo un máximo aprovechamiento y la mayor fidelidad posible en función de los ejercicios. Originalmente en su planificación no se esperaba conseguir un solo escenario capaz de dar soporte a la totalidad de los ejercicios, sino varios, no obstante, finalmente se consiguió y facilita la labor de configuración.
- Guardar y automatizar las configuraciones en función de los ejercicios que los alumnos deseen realizar, con el fin de que los usuarios puedan retomar su trabajo en posteriores sesiones sin perder progreso alguno en sus ejercicios.
- Servir de nexo a la hora de añadir este trabajo a la aplicación web final que recibirán los alumnos que deseen reforzar sus conocimientos.

Como siempre, y como suele ser habitual en este tipo de trabajos, la labor de documentación resulta vital y se basa en la mayoría de los conceptos aprendidos a lo largo de la carrera, como cabría esperar, mejorando sobre todo mis conocimientos sobre Cisco CCNA, y necesitando conocer algunos contenidos presentes en certificaciones superiores como CCNP. Igualmente, otros lenguajes como JAVA con extensiones como JSF y JPA, o SQL han estado también presentes a la hora de tomar decisiones entre todos los implicados en el departamento en la realización de este laboratorio remoto. Decisiones que se han podido ir tomando con tranquilidad mediante correo electrónico o en persona acudiendo al despacho de mi tutor sin problema alguno a la hora de comunicarnos.

Ciertamente, el trabajo se ha vivido como cualquier otra práctica o proyecto realizado anteriormente en la carrera. El trabajo ha sido realizado en las aulas públicas predispuestas por la Facultad y en mi propio hogar. Siempre que ha sido posible se ha acudido a la Facultad para tratar los temas de importancia junto a los tutores y miembros del departamento.

Al igual, el trato recibido por mi tutor ha sido realmente bueno y siempre ha sido posible concertar una cita con el o acudir a su despacho cuando tenía un problema. En general, las condiciones de trabajo han sido muy buenas y flexibles, creyendo bajo mi punto de vista, que han favorecido a la realización de este trabajo. Asimismo, Existe la posibilidad de que siga colaborando con la implantación y puesta en marcha de este proyecto, solucionando los problemas de integración que puedan surgir y realizando mejoras al mismo.

Pese a no ser un trabajo laboral como tal, está bien formar parte de un grupo de trabajo y tener unos objetivos que cumplir cada cierto periodo de tiempo, en cierto modo sirve para tener experiencia laboral y un primer contacto con lo que me espera cuando termine la carrera. Sin duda uno de los aspectos más satisfactorios e importantes del trabajo.

8. ANEXOS

El presente trabajo ha dejado algunos puntos sin abordar, que si bien han sido tratados y propuestos dentro del departamento, no se han podido llegar a completar por no requerir del tiempo suficiente para implementar soluciones no pensadas de forma inicial o por problemas a la hora de comprar nuevo hardware para el laboratorio.

Por ejemplo, nos encontramos con el problema de no poder guardar el estado de las interfaces o las VLANs, siendo necesario avisar al usuario para que sepa cuales ha de volver a configurar en otra futura sesión. Dentro del departamento creemos que esto se puede solucionar en el futuro guardando algunos ficheros disponibles en la flash de los equipos, además del de configuración inicial.

Otro problema es la necesidad de poder establecer un password recovery en alguno de los equipos, en el caso de que algo vaya mal, de forma remota sin necesidad de acudir con un PC y acceder físicamente mediante consola. Actualmente existen regletas como la "Aten PN9108 power over internet 8 puertos" que permite a los administradores y usuarios controlar la activación, desactivación y reactivación de cualquier dispositivo conectado desde cualquier ordenador.

Aten PN9108 power over internet 8 puertos.

El laboratorio actual puede ser utilizado por dos usuarios a la vez, es decir, uno en un kit y el otro en el otro kit disponible, no obstante, se puede pensar en intentar que un mayor número de usuarios accedan al laboratorio de forma simultánea en el futuro si se sigue mejorando el funcionamiento del laboratorio.

9. BIBLIOGRAFÍA

Trabajo realizado gracias a la siguiente documentación:

9.1 LIBROS

CISCO. Libro oficial de la certificación CCNA (100-101 y 200-101).
CISCO. Libro oficial de la certificación CCNA-S (640-554).

9.2 RECURSOS ONLINE

[1] Cisco. *CCNA Routing & Switching*. [Online]. Disponible en: http://www.cisco.com/web/learning/certifications/associate/ccna/index.html

[2] Cisco. *CCNA Security*. [Online]. Disponible en: http://www.cisco.com/web/learning/certifications/associate/ccna_security/index.html

[3] Escuela Técnica Superior de Ingenieros Informáticos. *Tecnologías de Red CISCO: CCNA.* [Online, formato .pdf]. Disponible en: http://www.fi.upm.es/docs/estudios/grado/1703_DLSIIS_TecnologiasRedCCNA_13-14.pdf

[4] Escuela Técnica Superior de Ingenieros Informáticos. *Redes y Comunicaciones.* [Online, formato .pdf]. Disponible en: https://www.fi.upm.es/docs/estudios/grado/1499_Guia_redes_de_computadores_2012-2013_a.pdf

[5] Escuela Técnica Superior de Ingenieros Informáticos. *Diseño y Seguridad de Redes.* [Online, formato .pdf]. Disponible en: http://www.fi.upm.es/docs/estudios/muii/1719_Diseno_Seguridad_de_Redes_13_14.pdf

[6] UPM. *Escuela Técnica Superior de Ingenieros Informáticos*. [Online]. Disponible en: http://www.fi.upm.es/

[7] M. J. Gañán. *Profesor titulado en la Escuela Técnica Superior de Ingenieros Informáticos*. [Página personal online]. Disponible en: http://conwet.fi.upm.es/es/people/miguel-jimenez

[8] Universidad Politécnica de Madrid. [Online]. Disponible en: http://www.upm.es/institucional

[9] Escuela Técnica Superior de Ingenieros Informáticos. *Página web de la asignatura de Redes de Computadores.* [Online]. Disponible en: http://www-lt.ls.fi.upm.es/redes_computadores/

[10] Escuela Técnica Superior de Ingenieros Informáticos. *Conwet Lab.* .[Online]. Disponible en: http://www.conwet.com/

[11] CISCO. *Cisco Packet Tracer*. [Online]. Disponible en: http://www.packettracernetwork.com/

[12] CISCO. *Cisco 2911 Integrated Services Router*. [Online]. Disponible en: http://www.cisco.com/c/en/us/products/routers/2911-integrated-services-router-isr/index.html

[13] CISCO. *Cisco 2911 Integrated Services Router SEC/K9.* [Online]. Disponible en: http://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

[14] CISCO. *Cisco Catalyst 2960-24TT-L Switch*. [Online]. Disponible en: http://www.cisco.com/c/en/us/support/switches/catalyst-2960-24tt-l-switch/model.html

[15] CISCO. *Cisco ASA 5500 Series Adaptive Security Appliances*. [Online]. Disponible en: http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/product_data_sheet0900aecd802930c5.html

[16] Wikipedia. *Definición de backup o copia de seguridad.* [Online]. Disponible en: http://es.wikipedia.org/wiki/Copia_de_seguridad

[17] Microsoft Office. *Herramienta Word*. [Online]. Disponible en: http://es.wikipedia.org/wiki/Microsoft_Word

[18] Microsoft Office. *Herramienta Excel*. [Online]. Disponible en: http://es.wikipedia.org/wiki/Microsoft_Excel

[19] Microsoft. *Herramienta Paint.* [Online]. Disponible en: http://es.wikipedia.org/wiki/Microsoft_Paint

[20] Tarjeta. *Tarjeta Access Server NM-16A/S de 16 puertos.* [Online]. Disponible en: http://www.cisco.com/c/en/us/products/collateral/routers/3600-series-multiservice-platforms/prod_qas09186a00801850cd.html

[21] Cableado. *CAB-OCTAL-ASYNC.* [Online]. Disponible en: http://www.cisco.com/c/en/us/support/docs/dial-access/asynchronous-connections/14958-24.html

[22] Cableado. *RJ-45.* [Online]. Disponible en: http://es.wikipedia.org/wiki/RJ-45

[23] SSH. *Definición Secure SHell.* [Online]. Disponible en: http://es.wikipedia.org/wiki/Secure_Shell

[24] Listas de Acceso. ACLs. [Online]. Disponible en: http://es.wikipedia.org/wiki/Lista_de_control_de_acceso

[25] Google Docs. *Descripción de la herramienta*. [Online]. Disponible en: http://es.wikipedia.org/wiki/Google_Drive#Google_Docs

[26] Google Drive. *Descripción de la herramienta*. [Online]. Disponible en: http://es.wikipedia.org/wiki/Google_Drive

[27] AFORTIC. *Información sobre laboratorios remotos*. [Online]. Disponible en: http://www.afortic.org/oferta-academica/cisco-netacad/laboratorio

[28] TEC de Monterrey. *Mejora al Proceso de Enseñanza-Aprendizaje Mediante el Acceso Remoto a Laboratorios de Redes*. [Online]. Disponible en: http://tical_2011.redclara.net/doc/Patricia_Chavez.pdf

[29] Universidad Nacional Abierta y a Distancia UNAD. *NETLAB.* [Online]. Disponible en: http://186.113.18.80/

[30] How to use SSH in a pc in packet tracer. *Linkedin* [Online]. Disponible en: http://www.linkedin.com/groups/How-use-SSH-in-pc-3796209.S.115327580

[31] Aplicación de AAA: Authentication, Authorization and Accounting. *Security Artwork*. [Online]. Disponible en:
http://www.securityartwork.es/2013/12/12/aplicacion-de-aaa-authentication-authorization-and-accounting/

[32] Autenticación de usuarios mediante un servidor AAA. *Youtube*. [Online]. Disponible en:
https://www.youtube.com/watch?v=mweuI-qAgXI

[33] Configuring TACACS+. *Cisco*. [Online]. Disponible en:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/sec_tacacsplus.html

[34] Configuring Local Authentication and Authorization. *Cisco*. [Online]. Disponible en:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01000.pdf

[35] Configuring Switch-Based Authentication. *Cisco*. [Online]. Disponible en:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swauthen.html

[36] Seguridad en el acceso a dispositivos Cisco. *BlogSpot*. [Online]. Disponible en:
http://librosnetworking.blogspot.com.es/2008/10/seguridad-en-el-acceso-dispositivos.html

[37] How to configure extended access list on router. *Computer networking notes*. [Online]. Disponible en:
http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/extended-access-list.html

[38] Configurar un Router-Switch Cisco para usar SSH en lugar de Telnet. *Rm-rf.es*. [Online]. Disponible en:
http://rm-rf.es/configurar-un-router-switch-cisco-para-usar-ssh-en-lugar-de-telnet/

[39] Como crear un usuario de solo lectura. *Soporte Cisco*. [Online]. Disponible en:
https://supportforums.cisco.com/es/discussion/11726941

[40] Configurar servidor AAA. *Todo sobre Packet Tracer*. [Online]. Disponible en: http://todopacketracer.wordpress.com/2012/03/16/configurar-servidor-aaa/

[41] Configuring Passwords and Privileges. *Cisco*. [Online]. Disponible en: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

[42] Passwords and Privileges Commands. *Cisco*. [Online]. Disponible en: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfpass.html

[43] Understand the levels of privilege in the Cisco IOS. *TechRepublic*. [Online]. Disponible en: http://www.techrepublic.com/blog/data-center/understand-the-levels-of-privilege-in-the-cisco-ios-104552/

[44] Restricting commands on a Cisco Router with Privilege Levels. *GIAC*. [Online]. Disponible en: http://www.giac.org/paper/gsec/419/restricting-commands-cisco-router-privilege-levels/101042

[45] Privilege Levels in Cisco IOS. *All abut networking*. [Online]. Disponible en: http://networkingtips-tricks.blogspot.com.es/2010/04/privilege-levels-in-cisco-ios.html

[46] Changing Privilege Levels For Cisco IOS Commands. *PacketU*. [Online]. Disponible en: http://www.packetu.com/2012/09/06/changing-privilege-levels-for-cisco-ios-commands/

[47] Privilege Levels. *Safari Books*. [Online]. Disponible en: https://www.safaribooksonline.com/library/view/hardening-cisco-routers/0596001665/ch04s07.html

[48] Cisco EEM Basic Overview and Sample Configurations. *Cisco soporte*. [Online]. Disponible en: https://supportforums.cisco.com/document/117596/cisco-eem-basic-overview-and-sample-configurations

[49] Event Manager (EEM). *Router Jockey*. [Online]. Disponible en http://routerjockey.com/2010/06/14/working-with-the-embedded-event-manager-eem/

[50] Multiple privilege levels. *Cisco Zine*. [Online]. Disponible en: http://www.ciscozine.com/multiple-privilege-levels/

[51] EEM Script. *Network Total*. [Online]. Disponible en: http://networkingtotaltutorials.blogspot.com.es/2013/03/eem-script_2263.html

[52] Configurando AAA en un router. *Netwrokeand.* [Online]. Disponible en: http://networkeando.blogspot.com.es/2009/01/configurando-aaa-en-un-router.html

[53] Seguridad de puerto en switches Cisco. *Mikroways*. [Online]. Disponible en: http://www.mikroways.net/2009/11/26/seguridad-de-puerto-en-switches-cisco/

[54] Understanding Cisco EEM by examples Part 2. *Cisco soporte*. [Online]. Disponible en: https://learningnetwork.cisco.com/docs/DOC-19468

[55] Como configurar Access Lists. *HighSec*. [Online]. Disponible en: http://highsec.es/2013/06/como-configurar-access-lists-firewall-integrado-de-un-router-cisco/

[56] Listas de Control de Acceso (ACLs). *Dituyi*. [Online]. Disponible en: http://www.dituyi.net/listas-de-control-de-acceso-acls/

[57] How to edit a Named Access Control List (ACL) on router. *OmniSecu*. [Online]. Disponible en: http://www.omnisecu.com/cisco-certified-network-associate-ccna/how-to-edit-a-named-access-control-list-acl-on-router.php

[58] Editar una ACL. *BroadBand*. [Online]. Disponible en: http://www.dslreports.com/faq/13793

Este documento esta firmado por

	**Firmante**	CN=tfgm.fi.upm.es, OU=CCFI, O=Facultad de Informatica - UPM, C=ES
	Fecha/Hora	Wed Jan 07 23:41:33 CET 2015
	Emisor del Certificado	EMAILADDRESS=camanager@fi.upm.es, CN=CA Facultad de Informatica, O=Facultad de Informatica - UPM, C=ES
	Numero de Serie	630
	Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)